CISCO SYSTEMS

Text Part Number: 78-6218-07 Rev. A0

Release Notes for Catalyst 6000 Family Software Release 5.x

Current Release (January 3, 2000)
5.3(4)CSX

Previous Releases
5.3(3)CSX, 5.3(2)CSX, 5.3(1a)CSX, 5.2(3)CSX, 5.2(2)CSX, 5.2(1)CSX, 5.1(1)CSX

Note   Release notes for prior Catalyst 6000 family software releases were accurate at the time of release. However, for information on the latest caveats and updates to previously released Catalyst 6000 family software releases, refer to the release notes for the latest maintenance release in your software release train. You can access all Catalyst 6000 family release notes at the World Wide Web locations listed in the "Cisco Connection Online" section on page 44.

Document Contents

This document consists of these sections:

Release 5.*x* Memory Requirements

Your Supervisor Engine 1 is shipped with 64-MB DRAM, which fully supports software release 5.*x*.

Product and Software Version Matrix

This section contains configuration matrixes to help you order Catalyst 6000 family products. Table 1 lists the minimum supervisor engine version and the current recommended/default supervisor engine software version for Catalyst 6000 family modules and chassis.

Note   There might be additional minimum software version requirements for intelligent modules (those that run an additional, separate software image). Refer to the software release notes for the module type for more information.

Table 1   **Minimum, Recommended, and Default Supervisor Engine Software Versions**

Product Number append with "=" for spares	Product Description	Minimum Supervisor Software Version	Recommended/Default Supervisor Software Version
Supervisor Engine 1			
WS-X6K-SUP1A-MSFC	Supervisor Engine 1, dual-port 1000BaseX uplinks, with enhanced QoS features, Policy Feature Card (PFC), and Multilayer Switch Feature Card (MSFC)[1]	5.3(1a)CSX	5.3(2)CSX
WS-X6K-SUP1A-PFC	Supervisor Engine 1, dual-port 1000BaseX uplinks, with enhanced QoS features, and Policy Feature Card[1]	5.3(1a)CSX	5.3(2)CSX
WS-X6K-SUP1A-2GE	Supervisor Engine 1, dual-port 1000BaseX uplinks, with enhanced QoS features	5.3(1a)CSX	5.3(2)CSX
WS-X6K-SUP1-2GE	Supervisor Engine 1, dual-port 1000BaseX uplinks	5.1(1)CSX	5.2(3)CSX

Table 1   Minimum, Recommended, and Default Supervisor Engine Software Versions (continued)

Product Number append with "=" for spares	Product Description	Minimum Supervisor Software Version	Recommended/Default Supervisor Software Version
Ethernet, Fast Ethernet, and Gigabit Ethernet			
WS-X6416-GE-MT	16-port Gigabit Ethernet MT-RJ with enhanced QoS features	5.3(1a)CSX	5.3(2)CSX
WS-X6408A-GBIC	8-port Gigabit Ethernet GBIC with enhanced QoS features	5.3(1a)CSX	5.3(2)CSX
WS-X6408-GBIC	8-port Gigabit Ethernet GBIC	5.1(1)CSX	5.2(3)CSX
WS-X6224A-100FX	24-port 100FX Multimode MT-RJ with enhanced QoS features	5.3(1a)CSX	5.3(2)CSX
WS-X6224-100FX-MT	24-port 100FX Multimode MT-RJ	5.1(1)CSX	5.2(3)CSX
WS-X6248A-RJ-45	48-port 10/100TX RJ-45 with enhanced QoS features	5.3(1a)CSX	5.3(2)CSX
WS-X6248-RJ-45	48-port 10/100TX RJ-45	5.1(1)CSX	5.2(3)CSX
WS-X6248A-TEL	48-Port 10/100TX RJ-21 with enhanced QoS features	5.3(1a)CSX	5.3(2)CSX
WS-X6248-TEL	48-Port 10/100TX RJ-21	5.2(1)CSX	5.2(3)CSX
WS-X6024-10FL-MT	24-port 10BaseFL MT-RJ with enhanced QoS features	5.3(3)CSX	5.3(3)CSX
ATM[2]			
WS-X6101-OC12-SMF	Single-port Single-Mode OC-12 ATM	5.3(2)CSX	5.3(2)CSX
WS-X6101-OC12-MMF	Single-port Multimode OC-12 ATM	5.3(2)CSX	5.3(2)CSX
Multilayer Switch Module (MSM)[3]			
WS-X6302-MSM	Multilayer Switch Module	5.2(1)CSX	5.2(3)CSX
Modular Chassis			
WS-C6009	Catalyst 6009 chassis (9-slot)	5.1(1)CSX	5.2(3)CSX
WS-C6509	Catalyst 6509 chassis (9-slot)	5.1(1)CSX	5.2(3)CSX
WS-C6006	Catalyst 6006 chassis (6-slot)	5.2(1)CSX	5.2(3)CSX
WS-C6506	Catalyst 6506 chassis (6-slot)	5.2(1)CSX	5.2(3)CSX

1 See the *Catalyst 6000 Family MSFC and PFC Configuration Guide*
2 See the *ATM Configuration Guide and Command Reference*
3 See the *Multilayer Switch Module Release Notes*

Orderable Software Images

Table 2 lists the software versions and applicable ordering information for the Catalyst 6000 family supervisor engine software.

Table 2   Orderable Software Images

Software Version	Filename	Orderable Product Number Flash on System	Orderable Product Number Spare Upgrade (Floppy Media)
Supervisor Engine 1			
5.3(4)CSX	cat6000-sup.5-3-4-CSX.bin	SFC6K-SUP-5.3.4-CSX	SWC6K-SUP-5.3.4-CSX=
5.3(3)CSX	cat6000-sup.5-3-3-CSX.bin	SFC6K-SUP-5.3.3-CSX	SWC6K-SUP-5.3.3-CSX=
5.3(2)CSX	cat6000-sup.5-3-2-CSX.bin	SFC6K-SUP-5.3.2-CSX	SWC6K-SUP-5.3.2-CSX=
5.2(3)CSX	cat6000-sup.5-2-3-CSX.bin	SFC6K-SUP-5.2.3-CSX	SWC6K-SUP-5.2.3-CSX=
5.2(2)CSX	cat6000-sup.5-2-2-CSX.bin	SFC6K-SUP-5.2.2-CSX	SWC6K-SUP-5.2.2-CSX=
5.2(1)CSX	cat6000-sup.5-2-1-CSX.bin	SFC6K-SUP-5.2.1-CSX	SWC6K-SUP-5.2.1-CSX=
5.1(1)CSX	cat6000-sup.5-1-1-CSX.bin	SFC6K-SUP-5.1.1-CSX	SWC6K-SUP-5.1.1-CSX=

Features for Supervisor Engine Software Release 5.3

This section describes the new features available in software release 5.3.

- UniDirectional Link Detection (UDLD) detects unidirectional connections on both copper and fiber-optic links.

- RADIUS authentication provides client-server authentication for users attempting to connect to the switch.

- Jumbo frame support for intra-VLAN traffic on Gigabit Ethernet links increases the MTU size to 9216 bytes (note that jumbo frames cannot be routed or fragmented for transmission through slower ports).

- Virtual Management Policy Server (VMPS) client support allows network administrators to define the VLAN membership policies for their network in a central database so that the switch automatically configures user ports to the correct VLAN.

- With the Single-Port OC-12 ATM Module (SMF or MMF):

  — Reassembly of up to 255 buffers simultaneously (each buffer represents a packet)

  — Support for up to 4096 virtual circuits

  — Support for AAL 5

  — ATM LANE 1.0, including LEC, LES, BUS, and LECS.

  — MPOA support

- On switches with a Policy Feature Card (PFC):

Note IPX VACLs, QoS ACLs, COPS-DS, and RSVP for Qualitative Service were introduced in software release 5.3(1a)CSX but were not fully tested; you were instructed not to use them. **These features can be used in software releases 5.3(3)CSX or later as they have been fully tested.**

— VLAN access control lists (VACLs) using IP, IPX, and MAC ACLs.

VACL enhancements in software release 5.3(3)CSX are as follows:

A VACL redirect ACE allows a unicast flow to be specified.

— Common Open Policy Service (COPS) for Differentiated Services (DS) allows QoS to be configured from a central policy decision point server.

— Resource reSerVation Protocol (RSVP) for Qualitative Service allows hosts to request QoS.

— Remote SPAN (RSPAN) supports source and destination SPAN ports on other compatible switches.

— Quality of service (QoS) supports classification, marking, and policing using IP, IPX, and MAC ACLs.

— Accelerated Server Load Balancing (ASLB) support enables Catalyst 6000 family switches to cache Cisco LocalDirector load balancing flows, accelerating the performance of the LocalDirector, which is a network appliance with a secure, real-time, embedded operating system that intelligently load balances IP traffic across multiple servers (see the *Catalyst 6000 Family Accelerated Server Load Balancing Installation and Configuration Note*).

ASLB enhancements in software release 5.3(3)CSX are as follows:

A TCP port can be a wildcard (0).

Up to 1024 virtual-IP addresses and TCP port pairs are supported.

Note Accelerated Server Load Balancing was previously called LocalDirector Accelerator in these release notes.

- On switches with a Multilayer Switch Feature Card (MSFC):

— IP Multilayer Switching (MLS) provides high-performance hardware-based Layer 3 switching of IP unicast traffic, offloading processor-intensive IP packet routing from network routers.

— IP Multicast Multilayer Switching (IP MMLS) provides high-performance hardware-based Layer 3 switching of IP multicast traffic, offloading processor-intensive IP multicast packet routing from network routers.

— IPX MLS provides high-performance hardware-based Layer 3 switching of IPX unicast traffic, offloading processor-intensive IPX packet routing from network routers.

— Standard and extended IOS access control lists (ACLs) at wire rate.

— Netflow Data Export (NDE) allows a summary of intersubnet Layer 3 traffic statistics for all expired flows to be periodically exported to a network management data collector.

Note Refer to the *Release Notes for Catalyst 6000 Family Multilayer Switch Feature Card* for more information.

Features for Supervisor Engine Software Release 5.2

This section describes the new features available in software release 5.2.

- GARP VLAN Registration Protocol (GVRP; see IEEE 802.1p) provides 802.1Q-compliant VLAN pruning and dynamic VLAN creation on 802.1Q trunk ports.

- GARP Multicast Registration Protocol (GMRP; see IEEE 802.1p) maintains Layer 2 multicast groups that determine which switch ports need to participate in multicasts.

- EtherChannel frame distribution is configurable with Layer 2 Switching Feature Card II (WS-F6020A) and can use either Media Access Control (MAC) addresses or IP addresses and either source or destination or both source and destination addresses.

  Enter a **show module** command for the supervisor engine to determine if EtherChannel frame distribution is configurable on your switch. If the display shows the "Sub-Type" to be "L2 Switching Engine I WS-F6020," then EtherChannel frame distribution is not configurable on your switch; it uses source and destination MAC addresses. EtherChannel frame distribution is configurable with any other switching engine and the default is to use source and destination IP addresses.

- The Spanning-Tree Protocol can be enabled and disabled on a per-VLAN basis.

Features for Supervisor Engine Software Release 5.1

This section describes the new features available in software release 5.1.

- IP supernetting, compatible with classless interdomain routing (CIDR) allows entry of a netmask instead of a subnet mask.

- 802.1Q-to-ISL VLAN mapping allows mapping of up to eight 802.1Q VLANs numbered above 1005 to ISL VLANs.

- Quality of service (QoS) prioritizes network traffic with class of service (CoS) values received in ISL or 802.1Q frame headers or with CoS values set in the switch.

- All Ethernet ports on all modules, including those on a standby supervisor engine, support EtherChannel (maximum of eight ports) with no requirement that ports be contiguous or on the same module.

- All Ethernet ports on all modules support Inter-Switch Link (ISL) and 802.1Q VLAN trunking.

- For transmitted traffic, provides up to four SPAN sessions; for received or both transmitted and received traffic, provides up to two SPAN sessions.

Usage Guidelines and Restrictions

This section provides usage guidelines and restrictions for the Catalyst 6000 family switches.

- The following **debounce timer** command options have been added to increase the jitter tolerance on 10/100 UTP ports to make them interoperable with out-of-spec NICs:

  set option debounce enable—sets debounce to 3.1 seconds on 10/100 cards.

  set option debounce disable—sets debounce to 300 mS. The default is 300 mS debounce. (CSCdp56343)

- Software release 5.*x* does not support full or destination-source flows for IPX traffic. As a result, please note that the following caveat listed as open in release 5.3(3) will not be fixed:

When you change an IPX flow to destination-source, the **show mls entry ipx destination** command used to specify a specific destination, displays all IPX Layer 3 entries rather than just those for a specific destination IPX address. (CSCdm46984)

- The following bug was mistakenly listed as open in software release 5.3(3)CSX. This bug never affected release 5.3(3)CSX or previous releases.

  Bug description: SNMP: A system reset might occur when generating TopN reports with portTopNMode set to portTopNForeground(1). The workaround is to set portTopNMode to portTopNBackground(2) for all entries in portTopNControlTable. (CSCdp27013)

- Please note that the following caveat, listed as open in previous releases, will not be fixed:

  Changing the console port baud rate from 19,200 to 38,400 incorrectly sets the console port to 9600 baud. After a reset, the console port baud rate is 38,400. Changing the rate to 38,400 from any other setting works correctly. (CSCdk86876)

- Please note that the following caveat, listed as open in release 5.3(3)CSX will not be fixed:

  You cannot use the tftpGrp MIB object to download Catalyst 6000 ATM software. (CSCdp16574)

- Use the QoS strict-priority queues only for your highest-priority traffic. The strict-priority queues are designed to accommodate only a limited volume of traffic. In switches with Supervisor Engine WS-X6K-SUP1-2GE, if you overload the strict-priority-queues, the supervisor engine cannot service the standard queues. (CSCdm90683)

- The following bug was mistakenly identified as having been fixed in software release 5.3(1a)CSX. **This bug was actually fixed prior to the 5.1(1)CSX software release and therefore was never an issue with Catalyst 6000 family switches.**

  Bug description: In some cases, a switch with redundant supervisor engines might reset as a result of the change from Daylight Saving Time to Standard Time. This problem only occurs if the Daylight Saving Time adjustment is enabled (using the **set summertime enable** command) and the switch has not been reset or power-cycled since the change to Standard Time. This problem is resolved in software release 5.3(1a)CSX. (CSCdk57762)

- You have to make sure that the redirect port defined in a VACL is on the same VLAN as the "incoming" VLAN for the packet that is to be redirected. Otherwise, the redirected packet will be dropped.

  For example, a redirect VACL is defined on VLAN 5 and the redirect destination port is also on VLAN 5. If an MLS entry is destined to VLAN 5, packets that are coming from VLAN 2 hit this MLS entry and also hit the VACL redirect ACE (both VLAN 2 and VLAN 5 ACLs will be checked) and are redirected in the incoming VLAN, VLAN 2. The redirect destination port will drop them since it is on VLAN 5 rather than on VLAN 2.

- With QoS disabled, a Gigabit EtherChannel can contain ports with both strict-priority queues and ports without strict-priority queues. With QoS enabled, a Gigabit EtherChannel cannot contain both port types. If you enable QoS, ports drop out of any Gigabit EtherChannels that contain both port types.

- When a multicast goes to both bridged and routed addresses and the multicast packets going to the routed addresses are Layer 3 switched and the multicast matches an ACL such that QoS should rewrite the ToS byte in the multicast packet, QoS rewrites the ToS byte for the multicast packets that are Layer 3 switched, but does not rewrite the ToS byte for the multicast packets that are bridged.

- To avoid the case where all traffic is out of profile, the burst size specified in a QoS policing rule must be at least as large as the maximum packet size permissible in the traffic to which the rule is applied.

- The **set port qos trust** command and the **trust-ipprec** and **trust-dscp** port keywords are not allowed on 10-, 10/100-, and 100 Mbps ports. Instead, configure ACLs with the **trust-cos**, **trust-dscp**, and **trust-ipprec** ACE keywords. Note that the **trust-cos** port keyword can be used on 10-, 10/100-, and 100 Mbps ports to enable receive queue drop thresholds.

- 24-port 100FX Switching Modules (WS-X6224-100FX-MT) with a hardware version of 1.1 or lower only support IEEE 802.1Q VLAN trunking; they do not support ISL trunking. Do not configure ISL trunks on 24-port 100FX Switching Modules (WS-X6224-100FX-MT) with a hardware version of 1.1 or lower. The restriction against ISL VLAN trunking is the only known problem with hardware version 1.1 or lower of these modules. If you do not require ISL VLAN trunking, these modules are fully functional. The ISL VLAN trunking problem has been corrected in hardware version 1.2 or later of these modules. If you wish to return a WS-X6224-100FX-MT module with a hardware version of 1.1 or lower, contact Cisco Systems. You can identify WS-X6224-100FX-MT hardware versions using one of the following two methods:

  — Command-line interface (CLI) method—Use the **show version** command to identify the hardware version of the WS-X6224-100FX-MT module as follows:

```
console> show version
< ... output truncated ... >
Mod Port Model              Serial #    Versions
--- ---- ------------------ ----------- ------------------------------------
< ... output truncated ... >
5   24   WS-X6224-100FX-MT  SAD02470006 Hw : 1.1
< ... output truncated ... >
console>
```

  The example shows a WS-X6224-100FX-MT module with a hardware version of 1.1; this version does not support ISL VLAN trunking.

  — Physical inspection method—Look for the part number is printed on a label on the outer edge of the component side of the module. Versions 73-3245-04 or lower do not support ISL trunking.

- There is a cabling issue with the 48-Port 10/100TX Switching Module (WS-X6248-TEL). The WS-X6248-TEL module RJ-21 connectors **do not** support Category 3 RJ-21 telco connectors and cabling. Using Category 3 connectors and cabling causes carrier sense errors. The module's connectors are keyed for Category 5 telco connectors and cables. You **must** use Category 5 RJ-21 telco connectors and cables.

- We recommend that you do not use more than 1500 multicast groups with GMRP. This restriction does not apply to IGMP.

Open and Resolved Caveats in Software Release 5.3(4)CSX

This section describes open and resolved caveats in supervisor engine software release 5.3(4)CSX.

Open Caveats in Software Release 5.3(4)CSX

This section describes open caveats in supervisor engine software release 5.3(4)CSX.

- If you remove a line module at the same time as you remove an active supervisor from a Catalyst 6000 family switch that is in a redundant supervisor configuration, the switch may become unreachable. To prevent this, wait at least 5 seconds after removing an active supervisor to allow the switchover to occur before you remove a line card (CSCdp59829)

- The ToS byte remains unchanged in bridged multicast packets when Multicast Multilayer Switching (MMLS) is enabled. The system does not support multiple, different rewrites for a single packet. The rewrite that is generated for multicast is a Layer 3 rewrite so there is no rewrite for the Layer 2 forwarding.

  For example, you have a multicast source in VLAN 13, a receiver in the same VLAN, and a QoS IP ACL configured and mapped to the source's ingress port that matches the traffic flow and specifies DSCP 31. When you disable the MMLS feature, the IP packets captured on the receiver's port contain a ToS byte of x7C (the expected result). When you enable the MMLS feature and establish a Layer 3 flow, the captured packet's ToS byte is unchanged from the value sent by the source. A ToS rewrite occurs on the replicated packets in the outgoing VLANs (other than VLAN 13). For the packets that are bridged in the same incoming VLAN, no ToS rewrite occurs. (CSCdm72364)

- The RSVP access control entry (ACE) does not attach over an EtherChannel port if the QoS policy for ports forming the channel are set at different times. The workaround is to execute the steps that cause the problem in a different order. Consider that ports 4/1-8 are to be channeled and have identical role combinations:

  — **set port qos 4/1 policy local**

  — **set qos acl map acl1 4/1**

  — **set qos policy cops**

  — **set port qos 4/1 policy cops**

  — **set port channel 4/1-8 des**

  The above sequence of steps causes the problem. The following fix ensures that you never map different ACLs to different ports which might channel together and later switch them to all map to the same ACL.

The fix involves performing an intermediate step, clearing the ACL mapping on the ports that have a different ACL mapping than the other ports, and mapping them to all have the same ACL before trying to channel them together (it is important to clear the older mapping first).

— **set port qos 4/1 policy local**

— **set qos acl map acl1 4/1**

— **set qos policy cops**

— **clear qos acl map acl1 4/1**

— **set port qos 4/1 policy cops**

— **set port channel 4/1-8 des**

(CSCdp26277)

- Rapidly disabling and enabling QoS with the policy source set to COPS might cause the switch to reset. The workaround is to wait approximately 30 seconds after disabling QoS before reenabling it when the QoS policy source had been set to COPS. (CSCdp32467)

- Online diagnostic failures are experienced on modules during bring up, online insertion, or module reset if the QoS default-action MAC ACL is reconfigured to include an aggregate policer with an action of drop. The system default does not include an aggregate policer in the default-action MAC ACL. The likelihood of the diagnostics failures increases as the amount of traffic being policed (dropped) by that aggregate policer increases. In general, as the rate value specified in the policer decreases and/or the amount of traffic matching all ACLs specifying that aggregate policer increases. (CSCdp15471)

- After setting the QoS policy source to local, you might need to wait approximately 20 seconds before the QoS policy source can be set back to COPS. (CSCdp34367)

- After clearing a COPS role or all COPS roles, the console might hang for approximately 20 seconds before showing that the roles cleared. (CSCdp34381)

- Occasionally, when a module is removed before it comes online (and before it is finished running diagnostics), memory corruption might occur. To avoid this problem, do not remove or reinsert a module during system power up and do not remove or reinsert a module before it comes online. (CSCdp27673) (CSCdp27562)

- On Catalyst 6000 switches with redundant supervisor engines (MSFC and PFC), after power cycling the system, some modules might show this message:

  `LC_DNLD_VERIFY: Error - Checksum verify fail` errors.

  Note that this bug has no impact and you should ignore these messages. (CSCdp06845)

- When you remove a module and then reinsert a different module, after using the **clear config** *mod_num* command on the newly inserted module, the first port on the module might be shown as *disabled* in the port status field. There are two workarounds: 1) Do a second **clear config** *mod_num.* 2) Do a **set port enable** on the first port. (CSCdp25328)

- On Catalyst 6000 switches with redundant supervisor engines (MSFC and PFC), the following bus ASIC sequence mismatch might occur during a switchover:

  `%SYS-1-MOD_SEQMISMATCH:Bus asic sequence mismatch occurred on module 7 (asic=1, srcidx=0x0, seq=0)`

  Note that this bug has no impact and you should ignore these messages.(CSCdp25633)

- In systems with redundant supervisor engines, after a switchover to the redundant supervisor engine, the following message might be reported to the console:

```
Got main interrupt val : 0x2
Interrupt in DBus Slave block: 0x200
Soft reset of titan : done
```

  Note that this bug has no impact and you should ignore these messages.(CSCdp03131)

- When you change an IPX flow to destination-source, the **show mls entry ipx destination** command used to specify a specific destination displays all IPX Layer 3 entries rather than just those for a specific destination IPX address. (CSCdm46984)

- In systems with redundant supervisor engines, occasionally during the removal of the active supervisor engine, a bus ASIC sequence error syslog message is reported to the console as follows:

```
%SYS-1-MOD_SEQMISMATCH:Bus asic sequence mismatch occurred on module 8
```

  Additionally, "CentauriInterrupt" and "perseus_intr_hdlr" syslog messages might be generated. These messages might be generated for some or all installed modules. Ignore these messages. (CSCdm01334)

Note   This problem also occurred after a system power up or a switchover to the redundant supervisor engine; these issues have been resolved in software release 5.3(3)CSX.

- Occasionally, removal or insertion of a module does not generate any syslog messages. (CSCdm63338)

- Enabling RSVP installs local ACLs when COPS is the policy and DSBM is enabled on the port. This problem is caused when you configure a port to have COPS policy instead of local NVRAM policy and then you enable DSBM. The workaround is to enable DSBM first and then change the policy to COPS. If the port policy is already COPS, toggle this configuration to avoid the problem described. (CSCdp52924)

Resolved Caveats in Software Release 5.3(4)CSX

This section describes resolved caveats in supervisor engine software release 5.3(4)CSX:

- When a lot of QoS and/or Security ACLs are configured on the switch, the switch may occasionally reset. This problem is resolved in software release 5.3(4)CSX. (CSCdp17331)

- When an RMON alarm is configured for ATM related MIB objects, the switch used to stop responding to SNMP requests. The workaround was to avoid configuring the RMON alarm on ATM related MIB objects or to reset the switch if the alarm was configured. This problem is resolved in software release 5.3(4)CSX. (CSCdp48766)

  Note that this is a global command that will affect all the 10/100 UTP modules in the switch and cause an increase of 3 seconds for reconvergence if you have other switches connected to these 10/100 UTP ports. Use this command only as a workaround for interoperating with out-of-spec NICs.

- The **clear configuration** command on the MSM does not properly clear the configuration of the trunk. Some of the trunk ports have VLAN 1 removed and some do not. This might prevent setting the port-channel with other MSM ports. The workaround is to reset the MSM module. This problem is resolved in software release 5.3(4)CSX. (CSCdp11427)

- Occasionally, after a system reset or power on, you will see that the standby supervisor engine shows 0 ports and the standby ports are not enabled. This problem might happen if one of the supervisor engine is approximately 20 seconds later than the other to begin booting the runtime image after a system reset or system power on. The workaround is to try to reset the standby supervisor engine from the active supervisor engine's console port. If that does not work or is not allowed, you must remove and reinsert the standby supervisor engine. This problem is resolved in software release 5.3(4)CSX. (CSCdp20622)

- When SPAN is configured with Etherchannel ports, the open sources might not be correct (based on Etherchannel status). This problem is resolved in software release 5.3(4)CSX. CSCdp23958

- The GBIC link status between two supervisor engines changes continually between link up and link down after a unidirectional link failure. This problem is resolved in software release 5.3(4)CSX. (CSCdp37412)

- The MSM Autostate feature is not shutting down MSM interfaces in a VLAN when the last external interface in the VLAN is disconnected. This problem is resolved in software release 5.3(4)CSX. (CSCdp34155)

- No registration was received from removed modules after a supervisor engine switchover. This problem is resolved in software release 5.3(4)CSX. (CSCdp34000)

- The routine GetNextUnicastEarlEntry() was designed to be used to search unicast MAC entries and then return the module and port number from which the MAC entry was learned. In the case of a multicast entry, or an entry having a flood index, you should skip the entry to avoid returning an invalid module and port number that SNMP cannot handle. This problem is resolved in software release 5.3(4)CSX. (CSCdp31964)

- The trunk is going up and down when the channel is in channel-on mode and the trunk is in non-negotiate mode. This problem is resolved in software release 5.3(4)CSX. (CSCdp32703)

- The switch might experience unexpected behavior if you configure 1024 different VIPs, producing a VACL with 4092 entries. A VACL of this size stresses the BDD library to the upper limits of memory usage.This problem is resolved in software release 5.3(4)CSX. (CSCdp32519)

- HSRP failed to route traffic to the trunk on the redundant router for one of five VLANs configured. This problem is resolved in software release 5.3(4)CSX. (CSCdp18397)

- If you add a new VLAN to the system, the CAM entries for this newly added VLAN for RSVP are not created. As a result, RSVP PATH messages coming in over the new VLAN are dropped. This problem is resolved in software release 5.3(4)CSX. CSCdp27505

- Gigabit Ethernet counters show incorrect values. This problem is resolved in software release 5.3(4)CSX. (CSCdp22433)

- Attachment of a dynamic RSVP ACL might cause a system reset. This problem is resolved in software release 5.3(4)CSX. (CSCdp31142)

- After modifying existing IP ACLs using a script to add a large number of ACEs, the microflow policers might stop working. This problem is resolved in software release 5.3(4). (CSCdp38913)

- Inconsistent channel-forming behavior occurs in PagP for ports that support the strict priority queue and ports that do not. This problem is resolved in software release 5.3(4)CSX. (CSCdp34951)

- The LED light remains on indicating link speed even when the link is down. This problem is resolved in software release 5.3(4)CSX. (CSCdp42337)

- The following sequence of events results in the loss of the ASLB configuration:

    (a) Configuring ASLB

(b)   Successfully committing the ASLB configuration

(c)   Modifying the configuration

(d)   Unsuccessfully committing the modified configuration

Step (d) results in an inconsistent state. In release 5.3(4)CSX, the configuration is restored to the original when the modified configuration is not successfully committed. This problem is resolved in software release 5.3(4)CSX. (SCdp42842)

- A race condition problem between DTP and VTP table checking caused VTP not to clear VLANs. This problem is resolved in software release 5.3(4)CSX. (CSCdp34876)

- MSFC generates MCAST-2-MAXGDALIMIT error messages with only 503 multicast entries. This problem is resolved in software release 5.3(4)CSX. (CSCdp36453)

- If you enable port security, a static CAM entry gets added and is marked as 'X' indicating security. Disabling security does not clear this CAM entry. Reboot also does not clear the entry. Capture shows CAM entries before and after enabling security and even after reboot. This problem is resolved in software release 5.3(4)CSX. (CSCdp31802)

Open and Resolved Caveats in Software Release 5.3(3)CSX

This section describes open and resolved caveats in supervisor engine software release 5.3(3)CSX.

Open Caveats in Software Release 5.3(3)CSX

This section describes open caveats in supervisor engine software release 5.3(3)CSX.

- The ToS byte remains unchanged in bridged multicast packets when Multicast Multilayer Switching (MMLS) is enabled. The system does not support multiple, different rewrites for a single packet. The rewrite that is generated for multicast is a Layer 3 rewrite so there is no rewrite for the Layer 2 forwarding.

  For example, there is a multicast source in VLAN 13 and a receiver in the same VLAN. There is a QoS IP ACL configured and mapped to the source's ingress port that matches the traffic flow and specifies DSCP 31. When the MMLS feature is disabled, the IP packets captured on the receiver's port contain a ToS byte of x7C (the expected result). When the MMLS feature is enabled and a Layer 3 flow is established, the captured packet's ToS byte is unchanged from the value sent by the source. There is a ToS rewrite on the replicated packets in the outgoing VLANs but for the packets that are bridged in the same incoming VLAN, there is no ToS rewrite. (CSCdm72364)

- Use the QoS strict-priority queues only for your highest-priority traffic. The strict-priority queues are designed to accommodate only a limited volume of traffic. In switches with Supervisor Engine WS-X6K-SUP1-2GE, if you overload the strict-priority-queues, the supervisor engine cannot service the standard queues. (CSCdm90683)

- RSVP access control entry (ACE) does not attach over an EtherChannel port if the QoS policy for ports forming the channel are set at different times. The workaround is to execute the steps which cause the problem in a different order. Consider that ports 4/1-8 are to be channeled and have identical role combinations:

  — **set port qos 4/1 policy local**

  — **set qos acl map acl1 4/1**

  — **set qos policy cops**

— **set port qos 4/1 policy cops**

— **set port channel 4/1-8 des**

The above sequence of steps causes the problem. The fix shown below ensures that you never map different ACLs to different ports which might channel together, and later switch them to all map to the same ACL.

As shown below, the fix involves performing an intermediate step, clearing the ACL mapping on the ports which have a different ACL mapping than the other ports and mapping them to all have the same ACL before trying to channel them together (it's important to clear the older mapping first).

— **set port qos 4/1 policy local**

— **set qos acl map acl1 4/1**

— **set qos policy cops**

— **clear qos acl map acl1 4/1**

— **set port qos 4/1 policy cops**

— **set port channel 4/1-8 des**

(CSCdp26277)

- Rapidly disabling and enabling QoS with policy source set to COPS might cause the switch to reset. The workaround is to wait approximately 30 seconds after disabling QoS before reenabling it when QoS policy source had been set to COPS. (CSCdp32467)

- Online diagnostic failures are experienced on modules during power up, online insertion, or module reset if the QoS default-action MAC ACL is reconfigured to include an aggregate policer with an action of drop. The system default does not include an aggregate policer in the default-action MAC ACL. The likelihood of the diagnostics failures increases as the amount of traffic being policed (dropped) by that aggregate policer increases. In general, that is as the rate value specified in the policer decreases and/or the amount of traffic matching all ACLs specifying that aggregate policer increases. (CSCdp15471)

- After setting the QoS policy source to local, you might need to wait approximately 20 seconds before the QoS policy source can be set back to COPS. (CSCdp34367)

- After clearing a COPS role or all COPS roles, the console might hang for approximately 20 seconds before showing that the roles cleared. (CSCdp34381)

- SNMP: A system reset might occur when generating TopN reports with portTopNMode set to portTopNForeground(1). The workaround is to set portTopNMode to portTopNBackground(2) for all entries in portTopNControlTable. (CSCdp27013)

- Occasionally, when a module is removed before it comes online (and before it is finished running diagnostics), memory corruption might occur. To avoid this problem, do not remove or reinsert a module during system power up and do not remove or reinsert a module before it comes online. (CSCdp27673) (CSCdp27562)

- The **clear configuration** command on the MSM does not properly clear the configuration of the trunk. Some of the trunk ports have VLAN 1 removed and some do not. This might prevent setting the port-channel with other MSM ports. The workaround is to reset the MSM module. (CSCdp11427)

- On Catalyst 6000 switches with redundant supervisor engines (MSFC and PFC), after power cycling the system some modules might show *LC_DNLD_VERIFY: Error - Checksum verify fail* errors.

Note that this bug has no impact on the system and these messages should be ignored. (CSCdp06845)

- Occasionally, after a system reset or power on, you will see that the standby supervisor engine shows 0 ports and the standby ports are not enabled. This problem might happen if one of the supervisors is approximately 20 seconds later than the other to begin booting the runtime image after a system reset or system power on. The workaround is to try to reset the standby supervisor engine from the active supervisor engine's console port. If that does not work, or is not allowed, you must remove and reinsert the standby supervisor engine. (CSCdp20622)

- When you remove a module and then reinsert a different module, after using the **clear config** *mod_num* command on the newly inserted module, the first port on the module might be shown as *disabled* in the port status field. There are two workarounds: 1) Do a second **clear config** *mod_num.* 2) Do a **set port enable** on the first port. (CSCdp25328)

- You cannot use the tftpGrp MIB object to download Catalyst 6000 ATM software. (CSCdp16574)

- On Catalyst 6000 switches with redundant supervisor engines (MSFC and PFC), the following bus ASIC sequence mismatch might occur during a switchover:

```
%SYS-1-MOD_SEQMISMATCH:Bus asic sequence mismatch occurred on module 7 (asic=1,
srcidx=0x0, seq=0)
```

Note that this bug has no impact on the system and these messages should be ignored. (CSCdp25633)

- Changing the console port baud rate from 19,200 to 38,400 incorrectly sets the console port to 9600 baud. After a reset, the console port baud rate is 38,400. Changing the rate to 38,400 from any other setting works correctly. (CSCdk86876)

- In systems with redundant supervisor engines, after a switchover to the redundant supervisor engine, the following message might be reported to the console:

```
Got main interrupt val : 0x2
Interrupt in DBus Slave block: 0x200
Soft reset of titan : done
```

Note that this bug has no impact on the system and these messages should be ignored. (CSCdp03131)

- When you change an IPX flow to destination-source, the **show mls entry ipx destination** command used to specify a specific destination, displays all IPX Layer 3 entries rather than just those for a specific destination IPX address. (CSCdm46984)

- In systems with redundant supervisor engines, occasionally during the removal of the active supervisor engine, a bus ASIC sequence error syslog message is reported to the console as follows:

```
%SYS-1-MOD_SEQMISMATCH:Bus asic sequence mismatch occurred on module 8
```

Additionally, "CentauriInterrupt" and "perseus_intr_hdlr" syslog messages might be generated. These messages might be generated for some or all installed modules. Ignore these messages. (CSCdm01334)

Note   This problem also occured after a system power up or a switchover to the redundant supervisor engine; these issues have been resolved in software release 5.3(3)CSX.

- Occasionally, removal or insertion of a module does not generate any SYSLOG messages. (CSCdm63338)

Resolved Caveats in Software Release 5.3(3)CSX

This section describes resolved caveats in supervisor engine software release 5.3(3)CSX:

- System power up time and redundant supervisor engine switchover time too slow. System bringup time and redundant supervisor engine switchover time have been improved. This problem is resolved in software release 5.3(3)CSX. (CSCdm83881)

- When protocol filtering is enabled, Multicast Multilayer Switching (MMLS) does not work. To use MMLS, do not enable protocol filtering. This problem is resolved in software release 5.3(3)CSX. (CSCdm91222)

- Occasionally, the system might hang when the Policy Feature Card (PFC) is booted. This problem is resolved in software release 5.3(3)CSX. (CSCdm92293)

- The following message should be displayed when you modify the QoS default IP ACL to use the **trust-cos** ACE keyword:

```
Warning: ACL trust-cos should only be used with ports that are also configured with
port trust=trust-cos.
```

This problem is resolved in software release 5.3(3)CSX. (CSCdm88257)

- The **set spantree disable all** and **enable all** commands take 3 to 5 minutes to complete if VTP pruning is enabled. To avoid the delay, disable VTP pruning before entering the command, and reenable it after the command is complete. This problem is resolved in software release 5.3(3)CSX. (CSCdm78945)

- If you enable or disable QoS before a module is reported as being online, diagnostics on some ports on the module may fail. This problem is resolved in software release 5.3(3)CSX. (CSCdm85315)

- The syntax of the **clear security acl map** command supports entry of a single VLAN number. Entering a **clear security acl map** command with a range of VLANs generates an incorrect "Invalid ACL Name" message. This problem is resolved in software release 5.3(3)CSX. (CSCdm89538)

- A QoS IP ACL can contain nine ACEs that use port operator parameters. If you attempt to add a tenth QoS IP ACE that uses a port operator parameter to an ACL, the following incorrect message is displayed:

```
Cannot configure more than 10 logical operators (gt, lt, eq, neq, range) in an IP ACL.
```

The message errors are that it should state 9 instead of 10 operators and should not include "eq" in the logical operator's list. This problem is resolved in software release 5.3(3)CSX. (CSCdm88490)

- Occasionally replacing an existing QoS ACL might fail with a **Cannot configure more than 10 logical operators message** when there are less than 10 logical operators in the new ACL. To workaround this problem, enter a **clear qos acl map** command to delete the old ACL and then create the new ACL. This problem is resolved in software release 5.3(3)CSX. (CSCdm88538)

- After bridged microflow policing has been enabled and QoS has applied microflow policing rules to bridged traffic in some VLANs, if you then disable bridged microflow policing, QoS continues to apply microflow policing rules to bridged traffic in those VLANs until the switch is reset. This problem is resolved in software release 5.3(3)CSX. (CSCdm88933)

- The usage display for the **clear qos acl map** command is:

```
Usage: clear qos acl map <acl_name> <mod_num/port_num|vlan>
       clear qos acl map <acl_name|mod_num/port_num|vlan|all>
```

  The second syntax form fails when entered with multiple port numbers or multiple VLAN numbers. This problem is resolved in software release 5.3(3)CSX. (CSCdm89542)

- Do not use Netflow Data Export (NDE) version 1 (the default NDE configuration is version 7). This problem is resolved in software release 5.3(3)CSX. (CSCdm89362)

- After a supervisor engine switchover, a supervisor engine port might go into a state where the port state is disabled in NVRAM. However, the firmware believes that the port is up and there is a link on the port. This problem is resolved in software release 5.3(3)CSX. (CSCdm84809)

- When you configure DNS on the switch and specify a hostname for the COPS server, the switch on reset prints the following to the console every time the COPS/RSVP connection manager tries to initiate a connection to the COPS server (workgroup-pc is the COPS server in this example):

```
Translating "workgroup-pc.cisco.com"...domain server (171.69.2.132) (198.92.30.32)
(171.69.2.81) Host name lookup failure

Translating "workgroup-pc.cisco.com"...domain server (171.69.2.132) (198.92.30.32)
(171.69.2.81) Host name lookup failure

Translating "workgroup-pc.cisco.com"...domain server (171.69.2.132) (198.92.30.32) [OK]
```

  This happens until the switch successfully connects to the COPS server. This problem is resolved in software release 5.3(3)CSX. (CSCdm87215)

- An eight-port channel might stop forwarding traffic after a port in the channel is disabled. This problem is resolved in software release 5.3(3)CSX. (CSCdm89990)

- Occasionally, after being turned off and back on several times, switches configured as VTP clients stop accepting VTP updates. This problem is resolved in software release 5.3(3)CSX. (CSCdm90300)

- After a switch reset, non-trunking ports are put to errdisabled on a VTP client when the VLAN is activated. For example, the switch is a VTP client with an ISL trunk to a neighboring VTP server. There is a non-trunk port, port 6/6, assigned to VLAN 13. It is configured for auto, negotiate. The link connects to a port on another switch, which is also auto, negotiate. When the VTP client switch is reset, the module (port 6/6) comes online and a link up is received. The port state shows inactive because the native VLAN is not active. When the ISL trunk is up and the VLANs are learned, port 6/6 joins the bridge but approximately 20 seconds later, a DTP link down message is written to the console. This problem is resolved in software release 5.3(3)CSX. (CSCdm82642)

- System might run out of memory if SNMP cseFlowMcastQueryEntry is repeatedly created and deleted. This problem is resolved in software release 5.3(3)CSX. (CSCdp00531)

- Using Ctrl-R (command recall) at the initial password prompt displays any part of the password already entered. For example, if the password is "worker" and you have typed the first three characters of the password, a Ctrl-R will display a line reading: "Enter Password: wor." If you have entered the entire password and walked away, anyone can type Ctrl-R and reveal the password. This affects both the physical console port and the telnet virtual console. Also, this is with no TACACS server (local passwords only) using the default configuration. It also only happens at the initial login password prompt - the enable command's password prompt does not exhibit the problem. This problem is resolved in software release 5.3(3)CSX. (CSCdm92441)

- When using TACACS+, if you open a telnet session to the switch and enter a username and close the telnet session without entering a password, the TACACS+ session from the switch to the TACACS+ server remains open. This problem is resolved in software release 5.3(3)CSX. (CSCdp02341)

- Avoid using Ctrl-C after entering the **configure network** command. Using Ctrl-C results in a command half completed which leaves the switch in an unknown state for that feature. This problem is resolved in software release 5.3(3)CSX. (CSCdm27473)

- The switch has been booted with a configuration that includes a QoS IP ACL. You then disable QoS, but when you issue a **set qos** bridged-microflow-policing command, the command completes without warning that QoS is disabled. This problem seems to only occur if the bridged packet microflow feature is already enabled.

  A second problem is when you issue a **show qos acl info** command; the ACL is displayed without a warning that QoS is disabled. This problem is resolved in software release 5.3(3)CSX. (CSCdm85903)

- SNMP traps might not be properly generated. This problem is resolved in software release 5.3(3)CSX. (CSCdm76987)

- A system reset might occur when traces are enabled and you attempt to do a TFTP activity such as downloading a configuration. This problem is resolved in software release 5.3(3)CSX. (CSCdm83928)

- A system reset might occur upon receiving invalid PVSTs and BPDU's on an EtherChannel. This problem is resolved in software release 5.3(3)CSX. (CSCdp07549)

- Packets are still classified with old DSCP value after the ACL has been updated. This problem is resolved in software release 5.3(3)CSX. (CSCdp10614)

- The system might reset when you try to set objects in ciscoFlashPartitioningTable. This problem has been fixed by not supporting this Table. This problem is resolved in software release 5.3(3)CSX. (CSCdp11615)

- SNMP: After you set rowStatus of an eventEntry to under_creation, any set/get the eventEntry might reset the system. This problem is resolved in software release 5.3(3)CSX. (CSCdp13317)

- Occasionally after system power up, display shows minor hardware problem for modules. This problem is resolved in software release 5.3(3)CSX. (CSCdp11646)

- After entering a **set boot config-register ignore-config** and resetting the switch, the switch comes back up and attempts to use BOOTP to obtain an IP address. When the BOOTP sending messages are printed to the console, they are followed by a message: bootp_send: sendto 51. This message indicates that the BOOTP send is failing. This problem is resolved in software release 5.3(3)CSX. (CSCdp19611)

- If you change port speed from 100Mbps to 10Mbps and then back to 100Mbps, port traffic might stop until you reset the module. This problem is resolved in software release 5.3(3)CSX. (CSCdp11730)

- A VTP client and a VTP server in the same VTP domain are separated by a VTP transparent mode switch that is not a member of any VTP domain. When the VTP client is reset, the client does not update its configuration after receiving a VTP update from the VTP server. This problem is resolved in software release 5.3(3)CSX. (CSCdp05027)

- VTP notifications are sent on wrong SCP SAP address for the ATM module. This problem is resolved in software release 5.3(3)CSX. (CSCdp24165)

- Occasionally after system power up, console display shows minor hardware problem for some modules. Additionally, after a switchover to the redundant supervisor engine, "Change Status" messages are displayed. This problem is resolved in software release 5.3(3)CSX. (CSCdp24868)

Open and Resolved Caveats in Software Release 5.3(2)CSX

This section describes open and resolved caveats in supervisor engine software release 5.3(2)CSX.

Open Caveats in Software Release 5.3(2)CSX

This section describes open caveats in supervisor engine software release 5.3(2)CSX.

- Online diagnostic failures are experienced on modules during bringup, online insertion, or module reset if the QoS default-action MAC ACL is reconfigured to include an aggregate policer with an action of drop. The system default does not include an aggregate policer in the default-action MAC ACL. The likelihood of the diagnostics failures increases as the amount of traffic being policed (dropped) by that aggregate policer increases. In general, that is as the rate value specified in the policer decreases and/or the amount of traffic matching all ACLs specifying that aggregate policer increases. (CSCdp15471)

- Changing the console port baud rate from 19,200 to 38,400 incorrectly sets the console port to 9600 baud. After a reset, the console port baud rate is 38,400. Changing the rate to 38,400 from any other setting works correctly. (CSCdk86876)

- In systems with redundant supervisor engines, occasionally during bootup or after a switchover to the redundant supervisor engine, a bus ASIC sequence error syslog message is reported to the console as follows:

```
%SYS-1-MOD_SEQMISMATCH:Bus asic sequence mismatch occurred on module 8
```

    Additionally, "CentauriInterrupt" and "perseus_intr_hdlr" syslog messages might be generated. These messages might be generated for some or all installed modules. Ignore these messages. (CSCdm01334)

- Occasionally, removal or insertion of a module does not generate any SYSLOG messages. (CSCdm63338)

- The **set spantree disable all** and **enable all** commands take 3 to 5 minutes to complete if VTP pruning is enabled. To avoid the delay, disable VTP pruning before entering the command, and reenable it after the command is complete. (CSCdm78945)

- If you enable or disable QoS before a module is reported as being online, diagnostics on some ports on the module may fail. (CSCdm85315)

- The following message should be displayed when you modify the QoS default IP ACL to use the **trust-cos** ACE keyword:

```
Warning: ACL trust-cos should only be used with ports that are also configured with
port trust=trust-cos.
```

    (CSCdm88257)

- A QoS IP ACL can contain nine ACEs that use port operator parameters. If you attempt to add a tenth QoS IP ACE that uses a port operator parameter to an ACL, the following incorrect message is displayed:

```
Cannot configure more than 10 logical operators (gt, lt, eq, neq, range) in an IP ACL.
```

The message errors are that it should state 9 instead of 10 operators and should not include "eq" in the logical operator's list. (CSCdm88490)

- Occasionally replacing an existing QoS ACL might fail with a **Cannot configure more than 10 logical operators message** when there are less than 10 logical operators in the new ACL. To workaround this problem, enter a **clear qos acl map** command to delete the old ACL and then create the new ACL. (CSCdm88538)

- When two MSFC modules are configured for HSRP and are configured as SPAN or RSPAN source ports, the ingress traffic to the MSFC might not be mirrored to the destination port after HSRP switchover or switchover to the redundant supervisor engine and MSFC. To workaround the problem, enter the **set span** or **set rspan** command again. (CSCdm88732)

- After bridged microflow policing has been enabled and QoS has applied microflow policing rules to bridged traffic in some VLANs, if you then disable bridged microflow policing, QoS continues to apply microflow policing rules to bridged traffic in those VLANs until the switch is reset. (CSCdm88933)

- The syntax of the **clear security acl map** command supports entry of a single VLAN number. Entering a **clear security acl map** command with a range of VLANs generates an incorrect "Invalid ACL Name" message. (CSCdm89538)

- The usage display for the **clear qos acl map** command is:

```
Usage: clear qos acl map <acl_name> <mod_num/port_num|vlan>
       clear qos acl map <acl_name|mod_num/port_num|vlan|all>
```

The second syntax form fails when entered with multiple port numbers or multiple VLAN numbers. (CSCdm89542)

- Occasionally, after being turned off and back on several times, switches configured as VTP clients stop accepting VTP updates. (CSCdm90300)

- Use the QoS strict-priority queues only for your highest-priority traffic. The strict-priority queues are designed to accommodate only a limited volume of traffic. In switches with Supervisor Engine WS-X6K-SUP1-2GE, if you overload the strict-priority-queues, the supervisor engine cannot service the standard queues. (CSCdm90683)

- When protocol filtering is enabled, Multicast Multilayer Switching (MMLS) does not work. To use MMLS, do not enable protocol filtering. (CSCdm91222)

Resolved Caveats in Software Release 5.3(2)CSX

This section describes resolved caveats in supervisor engine software release 5.3(2)CSX:

- ATM-related bug: Invalid CAM entries are created when MPOA is configured. This problem is resolved in software release 5.3(2)CSX. (CSCdm79162)

- ATM-related bug: The ATM module port cannot be set to VLAN-based QoS (**set port qos** *mod*/*port* **vlan-based** command fails) as a result QoS ACLs mapped to VLANs do not work on the ATM module. This problem is resolved in software release 5.3(2)CSX. (CSCdm79972)

- ATM-related bug: When the ATM module has PVC configured, after removing and reinserting the fiber-optic cable, the ATM port is not added back to the spanning tree of the VLAN corresponding to PVC. This problem is resolved in software release 5.3(2)CSX. (CSCdp03272)

- ATM-related bug: Dynamic entries for the ATM module are not handled properly by the supervisor engine. This problem is resolved in software release 5.3(2)CSX. (CSCdp04871)

- ATM-related bug: In a configuration of about 150 VLANs and with a lot of unresolved ARPs on the ATM module, the supervisor engine complains about the SCP queue being full. This problem is resolved in software release 5.3(2)CSX. (CSCdp05776)

- ATM-related bug: The ports of the ATM singlemode fiber-optic module are not added to the spanning tree. This problem is resolved in software release 5.3(2)CSX. (CSCdp06550)

- Bus-error exception when a Layer 2 multicast entry is both a multicast protocol configured entry and also a user configured entry. This exception *might* occur when the multicast protocol is trying to delete the entry. This problem is resolved in software release 5.3(2)CSX. (CSCdp06796)

- Memory leak might occur if entries were created in alarmTable. This problem is resolved in software release 5.3(2)CSX. (CSCdp03309)

- Addresses are not learned in some VLANs due to vlan-don't-learn bit being unintentionally enabled. This problem is resolved in software release 5.3(2)CSX. (CSCdp00634)

Open and Resolved Caveats in Software Release 5.3(1a)CSX

This section describes open and resolved caveats in supervisor engine software release 5.3(1a)CSX.

Open Caveats in Software Release 5.3(1a)CSX

This section describes open caveats in supervisor engine software release 5.3(1a)CSX:

- Changing the console port baud rate from 19,200 to 38,400 incorrectly sets the console port to 9600 baud. After a reset, the console port baud rate is 38,400. Changing the rate to 38,400 from any other setting works correctly. (CSCdk86876)

- In systems with redundant supervisor engines, occasionally during bootup or after a switchover to the redundant supervisor engine, a bus ASIC sequence error syslog message is reported to the console as follows:

```
%SYS-1-MOD_SEQMISMATCH:Bus asic sequence mismatch occurred on module 8
```

Additionally, "CentauriInterrupt" and "perseus_intr_hdlr" syslog messages might be generated. These messages might be generated for some or all installed modules. Ignore these messages. (CSCdm01334)

- Occasionally, removal or insertion of a module does not generate any SYSLOG messages. (CSCdm63338)

- The **set spantree disable all** and **enable all** commands take 3 to 5 minutes to complete if VTP pruning is enabled. To avoid the delay, disable VTP pruning before entering the command, and reenable it after the command is complete. (CSCdm78945)

- If you enable or disable QoS before a module is reported as being online, diagnostics on some ports on the module may fail. (CSCdm85315)

- The following message should be displayed when you modify the QoS default IP ACL to use the **trust-cos** ACE keyword:

```
Warning: ACL trust-cos should only be used with ports that are also configured with
port trust=trust-cos.
```

(CSCdm88257)

- A QoS IP ACL can contain nine ACEs that use port operator parameters. If you attempt to add a tenth QoS IP ACE that uses a port operator parameter to an ACL, the following incorrect message is displayed:

  ```
  Cannot configure more than 10 logical operators (gt, lt, eq, neq, range) in an IP ACL.
  ```

  The message errors are that it should state 9 instead of 10 operators and should not include "eq" in the logical operator's list. (CSCdm88490)

- Occasionally replacing an existing QoS ACL might fail with a **Cannot configure more than 10 logical operators message** when there are less than 10 logical operators in the new ACL. To workaround this problem, enter a **clear qos acl map** command to delete the old ACL and then create the new ACL. (CSCdm88538)

- When two MSFC modules are configured for HSRP and are configured as SPAN or RSPAN source ports, the ingress traffic to the MSFC might not be mirrored to the destination port after HSRP switchover or switchover to the redundant supervisor engine and MSFC. To workaround the problem, enter the **set span** or **set rspan** command again. (CSCdm88732)

- After bridged microflow policing has been enabled and QoS has applied microflow policing rules to bridged traffic in some VLANs, if you then disable bridged microflow policing, QoS continues to apply microflow policing rules to bridged traffic in those VLANs until the switch is reset. (CSCdm88933)

- The syntax of the **clear security acl map** command supports entry of a single VLAN number. Entering a **clear security acl map** command with a range of VLANs generates an incorrect "Invalid ACL Name" message. (CSCdm89538)

- The usage display for the **clear qos acl map** command is:

  ```
  Usage: clear qos acl map <acl_name> <mod_num/port_num|vlan>
         clear qos acl map <acl_name|mod_num/port_num|vlan|all>
  ```

  The second syntax form fails when entered with multiple port numbers or multiple VLAN numbers. (CSCdm89542)

- Occasionally, after being turned off and back on several times, switches configured as VTP clients stop accepting VTP updates. (CSCdm90300)

- Use the QoS strict-priority queues only for your highest-priority traffic. The strict-priority queues are designed to accommodate only a limited volume of traffic. In switches with Supervisor Engine WS-X6K-SUP1-2GE, if you overload the strict-priority-queues, the supervisor engine cannot service the standard queues. (CSCdm90683)

- When protocol filtering is enabled, Multicast Multilayer Switching (MMLS) does not work. To use MMLS, do not enable protocol filtering. (CSCdm91222)

Resolved Caveats in Software Release 5.3(1a)CSX

This section describes resolved caveats in supervisor engine software release 5.3(1a)CSX:

- In some cases, you cannot remove a UGHD (up, gateway, host, dynamic) route from the switch IP routing table. This problem is resolved in software release 5.3(1a)CSX. (CSCdk14130)

- Configuring an ISL trunk on a root bridge switch with spanning tree on many VLANs can cause delays in BPDU transmission from that switch, which can cause all the non-root bridges in the network to expire their message age timers, which may cause brief periods of network instability. This problem is fixed in software release 5.3(1a)CSX. (CSCdk69087)

- If traffic is received through a port that has port security enabled before the port is in the forwarding state, the port is shutdown. This problem is fixed in software release 5.3(1a)CSX. (CSCdk73206)

- If the switch is in VTP client mode, entry of a **copy** *device:filename* **config** command may generate messages about nonexistent VLANs. Wait until the **show vlan** command displays the VLANs and then enter the **copy** command again. This problem is fixed in software release 5.3(1a)CSX. (CSCdm07337)

- In some cases, on a switch with both BackboneFast and UplinkFast enabled, the show spantree mod_num/port_num output shows that a port is in forwarding mode, but in reality the port is in listening mode. As a result, all data traffic received on the port is discarded. The workaround is to disable and reenable the affected port. This problem is resolved in software release 5.3(1a)CSX. (CSCdm08504)

- password authentication (without TACACS) can be slow when DNS is enabled and DNS server IP address is configured, but the DNS server is not reachable. The workaround is to disable DNS. This problem is resolved in software release 5.3(1a)CSX. (CSCdm14239)

- A module may report "Unknown GBIC" in the type field when HP GBIC(1000BASE-SX 30-0759-01) is installed. This problem is resolved in software release 5.3(1a)CSX. (CSCdm14762)

- Do not configure any module so that the number of GVRP-enabled ports, including the individual physical ports in GVRP-enabled EtherChannels, times the number of VLANs on the module, exceeds 720. This problem is fixed in software release 5.3(1a)CSX. (CSCdm18614; CSCdm18380)

- The MSM is not supported as a SPAN source port. Configuring the MSM as a SPAN source port generates a "Failed to configure source port" message. If you configure the MSM as a SPAN source port, all subsequent SPAN source port configuration commands for that SPAN session generate the same message until you remove the MSM from the source port list with a **set span disable** *mod_num/port_num* command. This problem is fixed in software release 5.3(1a)CSX. (CSCdm20365)

- When you turn off the power on any module, you cannot turn the power back on through SNMP. The workaround is to use the CLI command **set module power up** *mod_num*. This problem is fixed in software release 5.3(1a)CSX. (CSCdm23288)

- In some cases, when the active link of an UplinkFast link pair is disconnected, the switch does not transmit broadcast frames on the secondary link. This problem is resolved in software release 5.3(1a)CSX. (CSCdm23587)

- Occasionally, the switch shuts down in response to an erroneous over-temperature reading. This problem is resolved in software release 5.3(1a)CSX. (CSCdm24976)

- In some cases, if the primary UplinkFast link goes down, when it comes back up it can take 20 to 25 seconds to begin forwarding traffic instead of the usual one to five seconds, depending on the remote hardware. The workaround is to connect to a different port on the remote device if the problem occurs. This problem is resolved in software release 5.3(1a)CSX. (CSCdm26273)

- In some cases, UplinkFast might not function correctly between a Catalyst 6000 family switch and a Catalyst 4000 family switch, a Catalyst 2948G switch, or a Catalyst 5000 family Gigabit EtherChannel module (WS-X5410). This problem is resolved in software release 5.3(1a)CSX. (CSCdm34341)

- This bug does not effect system operation. The 48-Port 10/100TX Switching Modules (WS-X6248-TEL and WS-X6248-RJ-45) "Send admin" flow control field **(show port flowcontrol** *mod_num/port_num*) might show "desired" when the port is connected as well as when it is not connected or disabled. This problem is fixed in software release 5.3(1a)CSX. (CSCdm37747)

- If Gigabit channel ports and 10/100BaseTX channel ports are used as SPAN source ports, the Gigabit channel ports might not show up in the **Oper Source** ports field. This problem is fixed in software release 5.3(1a)CSX. (CSCdm39024)

- This bug does not effect system operation. On disabling the Multilayer Switch Module (MSM), the **show module** command shows "faulty" instead of "disabled". This problem is fixed in software release 5.3(1a)CSX. (CSCdm42419)

- Occasionally, disabling GVRP caused an exception. This problem is fixed in software release 5.3(1a)CSX. (CSCdm44130)

- If all ports of a channel are disturbed by either resetting the module(s) on the remote end, or due to a broadcast storm, the switch might not transmit or receive any GMRP control packets. The workaround is to disable and then enable the GMRP feature on the switch which experiences this problem. This problem is fixed in software release 5.3(1a)CSX. (CSCdm45744)

- If you delete the RMON alarmEntry or if you modify the alarmVariable of the RMON alarmEntry while that alarmVariable is being sampled, the switch might reset. This problem is resolved in software release 5.3(1a)CSX. (CSCdm49575)

- TACACS cannot control access to the switch based on the host's IP address. This problem is resolved in software release 5.3(1a)CSX. (CSCdm60984)

- A syslog message for a given facility is not sent to the syslog server if the syslog server severity level is set to a value equal to or greater than the message severity but the default severity level for that facility is set to a value less than the message severity. The workaround is to set the default facility severity level to a value equal to or greater than the configured syslog severity level. In release 5.3(1a)CSX, syslog messages are sent to the syslog server if the syslog server severity level is equal to or greater than the message severity and the default facility severity level is equal to or greater than the message severity. (CSCdm71889)

Open and Resolved Caveats in Software Release 5.2(3)CSX

This section describes open and resolved caveats in supervisor engine software release 5.2(3)CSX.

Open Caveats in Software Release 5.2(3)CSX

This section describes open caveats in supervisor engine software release 5.2(3)CSX:

- Changing the console port baud rate from 19,200 to 38,400 incorrectly sets the console port to 9600 baud. After a reset, the console port baud rate is 38,400. Changing the rate to 38,400 from any other setting works correctly. (CSCdk86876)

- In systems with redundant supervisor engines, occasionally during bootup or after a switchover to the redundant supervisor engine, a bus ASIC sequence error syslog message is reported to the console as follows:

```
%SYS-1-MOD_SEQMISMATCH:Bus asic sequence mismatch occurred on module 8
```

This message might be generated for some or all installed modules. Ignore this message. (CSCdm01334)

- If the switch is in VTP client mode, entry of a **copy** *device:filename* **config** command may generate messages about nonexistent VLANs. Wait until the **show vlan** command displays the VLANs and then enter the **copy** command again. This problem is fixed in software release 5.3(1)CSX. (CSCdm07337)

- Do not configure any module so that the number of GVRP-enabled ports, including the individual physical ports in GVRP-enabled EtherChannels, times the number of VLANs on the module, exceeds 720. This problem is fixed in software release 5.3(1)CSX. (CSCdm18614)

- The MSM is not supported as a SPAN source port. Configuring the MSM as a SPAN source port generates a "Failed to configure source port" message. If you configure the MSM as a SPAN source port, all subsequent SPAN source port configuration commands for that SPAN session generate the same message until you remove the MSM from the source port list with a **set span disable** *mod_num/port_num* command. This problem is fixed in software release 5.3(1)CSX. (CSCdm20365)

- When you turn off the power on any module, you cannot turn the power back on through SNMP. The workaround is to use the CLI command **set module power up** *mod_num.* This problem is fixed in software release 5.3(1)CSX. (CSCdm23288)

- Occasionally during bootup, a bus ASIC sequence error syslog message is reported to the console as follows:

```
%SYS-1-MOD_INVALIDSEQ:Bus asic invalid sequence occurred on module 3 (asic=1,
srcidx=0x0, seq=28)
```

  This message might be generated for any module. Ignore this message. This problem is fixed in software release 5.3(1)CSX. (CSCdm32301)

- This bug does not effect system operation. The 48-Port 10/100TX Switching Modules (WS-X6248-TEL and WS-X6248-RJ-45) "Send admin" flow control field **(show port flowcontrol** *mod_num/port_num*) might show "desired" when the port is connected as well as when it is not connected or disabled. This problem is fixed in software release 5.3(1)CSX. (CSCdm37747)

- If Gigabit channel ports and 10/100BaseTX channel ports are used as SPAN source ports, the Gigabit channel ports might not show up in the **Oper Source** ports field. This problem is fixed in software release 5.3(1)CSX. (CSCdm39024)

- This bug does not effect system operation. On disabling the Multilayer Switch Module (MSM), the **show module** command shows "faulty" instead of "disabled". This problem is fixed in software release 5.3(1)CSX. (CSCdm42419)

- If all ports of a channel are disturbed by either resetting the module(s) on the remote end, or due to a broadcast storm, the switch might not transmit or receive any GMRP control packets. The workaround is to disable and then enable the GMRP feature on the switch which experiences this problem. This problem is fixed in software release 5.3(1)CSX. (CSCdm45744)

Resolved Caveats in Software Release 5.2(3)CSX

This section describes resolved caveats in supervisor engine software release 5.2(3)CSX.

- Occasionally during bootup, a bus ASIC sequence error syslog message is reported to the console as follows:

```
%SYS-1-MOD_INVALIDSEQ:Bus asic invalid sequence occurred on module 3 (asic=1,
srcidx=0x0, seq=28)
```

  This message might be generated for any module. Ignore this message. This problem is fixed in software release 5.3(1)CSX. (CSCdm32301)

- When a port goes into the **errdisable** state, it may cause the MAC addresses of other devices to be learned from the port that is in the **errdisable** state. This problem is fixed in software release 5.2(3)CSX. (CSCdm48887)

- Occasionally, SNMP cannot access the **ifDescriptors** of some modules. This problem is fixed in software release 5.2(3)CSX. (CSCdm48259)

- When you hot-insert an MSM module into a chassis with minimal unused power capacity, the switch might reset. This problem is fixed in software release 5.2(3)CSX. (CSCdm53061)

- If a gigabit Ethernet port is briefly disconnected, it might show as **not connected** when it actually is. This problem is fixed in software release 5.2(3)CSX. (CSCdm60378)

- When resetting a Catalyst 2900XL switch that has a Gigabit Ethernet connection between a 2931-XL module and a WS-X6408-GBIC module in a Catalyst 6000 family switch, the connection might not reestablish. This problem is fixed in software release 5.2(3)CSX. (CSCdm80035)

- Occasionally, no RMON alarms are generated. This problem is fixed in software release 5.2(3)CSX. (CSCdm84753)

- Occasionally, host NICs connected to WS-X6248-TEL or WS-X6248-RJ-45 modules may incorrectly revert to half-duplex after an auto-negotiation failure. This problem is fixed in software release 5.2(3)CSX. (CSCdm88013)

Open and Resolved Caveats in Software Release 5.2(2)CSX

This section describes open and resolved caveats in supervisor engine software release 5.2(2)CSX.

Open Caveats in Software Release 5.2(2)CSX

This section describes open caveats in supervisor engine software release 5.2(2)CSX:

- Changing the console port baud rate from 19,200 to 38,400 incorrectly sets the console port to 9600 baud. After a reset, the console port baud rate is 38,400. Changing the rate to 38,400 from any other setting works correctly. (CSCdk86876)

- In systems with redundant supervisor engines, occasionally during bootup or after a switchover to the redundant supervisor engine, a bus ASIC sequence error syslog message is reported to the console as follows:

```
%SYS-1-MOD_SEQMISMATCH:Bus asic sequence mismatch occurred on module 8
```

  This message might be generated for some or all installed modules. Ignore this message. (CSCdm01334)

- If the switch is in VTP client mode, entry of a **copy** *device:filename* **config** command may generate messages about nonexistent VLANs. Wait until the **show vlan** command displays the VLANs and then enter the **copy** command again. This problem is fixed in software release 5.3(1)CSX. (CSCdm07337)

- Do not configure any module so that the number of GVRP-enabled ports, including the individual physical ports in GVRP-enabled EtherChannels, times the number of VLANs on the module, exceeds 720. This problem is fixed in software release 5.3(1)CSX. (CSCdm18614)

- The MSM is not supported as a SPAN source port. Configuring the MSM as a SPAN source port generates a "Failed to configure source port" message. If you configure the MSM as a SPAN source port, all subsequent SPAN source port configuration commands for that SPAN session

generate the same message until you remove the MSM from the source port list with a **set span disable** *mod_num/port_num* command. This problem is fixed in software release 5.3(1)CSX. (CSCdm20365)

- When you turn off the power on any module, you cannot turn the power back on through SNMP. The workaround is to use the CLI command **set module power up** *mod_num.* This problem is fixed in software release 5.3(1)CSX. (CSCdm23288)

- Occasionally during bootup, a bus ASIC sequence error syslog message is reported to the console as follows:

```
%SYS-1-MOD_INVALIDSEQ:Bus asic invalid sequence occured on module 3 (asic=1,
srcidx=0x0, seq=28)
```

This message might be generated for any module. Ignore this message. This problem is fixed in software release 5.3(1)CSX. (CSCdm32301)

- This bug does not effect system operation. The 48-Port 10/100TX Switching Modules (WS-X6248-TEL and WS-X6248-RJ-45) "Send admin" flow control field **(show port flowcontrol** *mod_num/port_num*) might show "desired" when the port is connected as well as when it is not connected or disabled. This problem is fixed in software release 5.3(1)CSX. (CSCdm37747)

- If Gigabit channel ports and 10/100BaseTX channel ports are used as SPAN source ports, the Gigabit channel ports might not show up in the **Oper Source** ports field. This problem is fixed in software release 5.3(1)CSX. (CSCdm39024)

- This bug does not effect system operation. On disabling the Multilayer Switch Module (MSM), the **show module** command shows "faulty" instead of "disabled". This problem is fixed in software release 5.3(1)CSX. (CSCdm42419)

- If all ports of a channel are disturbed by either resetting the module(s) on the remote end, or due to a broadcast storm, the switch might not transmit or receive any GMRP control packets. The workaround is to disable and then enable the GMRP feature on the switch which experiences this problem. This problem is fixed in software release 5.3(1)CSX. (CSCdm45744)

Resolved Caveats in Software Release 5.2(2)CSX

This section describes resolved caveats in supervisor engine software release 5.2(2)CSX.

- If the software image on the MSM is not bootable, contact Cisco's Technical Assistance Center (TAC) at 800 553-2447, 408 526-7209, or tac@cisco.com. This problem is fixed in software release 5.2(2)CSX. (CSCdm03564)

- There was a restriction that did not allow changing the native VLAN for ISL trunk ports. This restriction has been removed for non-dot1q trunking. This problem is fixed in software release 5.2(2)CSX. (CSCdm08306)

- When the last port in a VLAN that is actively participating in GMRP gets removed, the switch might experience a reset. This problem is fixed in software release 5.2(2)CSX. (CSCdm11116)

- If the software configuration register in the MSM is set to 0x2000 and the image specified using the **boot system flash sup-slot0:** [*filename*] command is not found, the MSM will sleep for more than 256 seconds before giving up the netboot and attempting to boot the image in the local bootflash instead. However, the supervisor engine resets the MSM before the 256 seconds is up. This problem is fixed in software release 5.2(2)CSX. (CSCdm15737)

- If protocol filtering is configured for an EtherChannel before the channel forms, it works correctly. If you configure protocol filtering after the channel has formed, it may not work correctly for transmitted traffic. This problem is fixed in software release 5.2(2)CSX. (CSCdm16439)

- On switches with more than 100 VLANs, after removing a module or entering a **set module power down** command, wait at least 60 seconds before putting the module back into service, either by reinserting it or by entering a **set module power up** command. This problem is fixed in software release 5.2(2)CSX. (CSCdm19125)

- The supervisor engine software incorrectly allows configuration of the MSM as a SPAN destination port. When configured as a SPAN destination port, the MSM ignores the SPAN traffic. If you configure an MSM as a SPAN destination port, remove it from the destination port list with the **set span disable** *mod_num/port_num* command. This problem is fixed in software release 5.2(2)CSX. (CSCdm20714)

- When the SPAN destination port is a trunk port, the encapsulation matches the trunk type: ISL or 802.1Q. When the SPAN destination port is an access port, the default encapsulation is 802.1Q. The default encapsulation cannot be changed on Gigabit Ethernet access ports used as a SPAN destination. To disable 802.1Q encapsulation on other ports, enter a **set trunk** *mod_num*/*port_num* **off** command before entering a **set span** command. This problem is fixed in software release 5.2(2)CSX. (CSCdm20968)

- When VTP Pruning is enabled, some VLANs that show as Pruned by VTP Pruning might be treated as joined by GVRP so that GVRP declares those VLANs on all of the GVRP-enabled trunks. This problem is fixed in software release 5.2(2)CSX. (CSCdm21455)

- The WS-X6248-TEL module spanning tree state shows forwarding but is not able to switch any traffic. This problem is fixed in software release 5.2(2)CSX. (CSCdm21520)

- On EtherChannels between 10/100 Ethernet switching modules, occasionally after changing the speed of the EtherChannel ports from 10 Mbps to 100 Mbps or 100 Mbps to 10 Mbps, the channel may form with fewer ports or multiple channels may form. To restore the original EtherChannel configuration, disable all the ports in the EtherChannel and then enable them. This problem is fixed in software release 5.2(2)CSX. (CSCdm22352)

- With redundant supervisor engines, after switch over to the standby supervisor engine, SNMP applications on network management systems fail when accessing cdpCacheTable (1.3.6.1.4.1.9.9.23.1.2.1). This problem is fixed in software release 5.2(2)CSX. (CSCdm22434)

- The **show config** command does not have the SPAN create option if multiple SPAN sessions have been created. If a configuration file is sourced via the configure command, only the last SPAN session ends up being created. This problem is fixed in software release 5.2(2)CSX. (CSCdm23199)

- On 10/100 and 100 Mbps Ethernet switching modules with one or more EtherChannel trunks, after entering **set module power down** and **set module power up** commands, occasionally the spanning tree state is "not connected" for all but VLAN 1. To restore connectivity, reset the module. This problem is fixed in software release 5.2(2)CSX. (CSCdm23329)

- When using the **set port speed** command to change from 100 to auto, channels on the port might split. This problem is fixed in software release 5.2(2)CSX. (CSCdm23529)

- If IGMP is enabled, when a port in an EtherChannel to the MSM gets disabled, the switch stops forwarding IP multicast traffic in groups learned on the switch to the MSM. To restore transmission of IP multicast traffic to the MSM, disable and then enable the channel. This problem is fixed in software release 5.2(2)CSX. (CSCdm24673)

- When you enter the **show sprom chassis** command, incorrect snmpOID and stackmib_oid values might be displayed. This problem is fixed in software release 5.2(2)CSX. (CSCdm26092)

- Because of a race condition when 10/100 ports are trunking and channeling, all VLANs are not added to the spanning tree except the native VLAN. This problem is fixed in software release 5.2(2)CSX. (CSCdm26399)

- When accessing the MSM through the **session** command, a timeout occurs when uploading an image from MSM bootflash to supervisor engine slot 0 (sup-slot0). This problem does not occur when connected to the MSM console port. This problem is fixed in software release 5.2(2)CSX. (CSCdm26984)

- When GMRP is learning a lot of groups the system might experience a reset while transmitting GMRP packets. This problem is fixed in software release 5.2(2)CSX. (CSCdm27226)

- It takes a long time to process the **set module power down** command for an MSM with a large number of VLANs (approximately 100 or more). This problem is fixed in software release 5.2(2)CSX. (CSCdm27592)

- Improved supervisor engine switchover for redundant supervisors. The time during supervisor failover in which packet forwarding has stopped has been greatly reduced with maintenance release 5.2(2)CSX. Previous version 5.2(1)CSX failover times were 30 to 60 seconds. With this maintenance release 5.2(2)CSX, supervisor failover is reduced to 3 to 10 seconds to resume packet forwarding. Both times are with spanning tree portfast enabled. See configuration information on spanning tree portfast. This problem is fixed in software release 5.2(2)CSX. (CSCdm27781)

- When QoS is enabled, a channel is not formed for ports configured with desirable or on mode and with different QoS values. But when QoS is disabled, the different QoS-value ports form a channel in on mode, but do not form a channel in desirable mode.This problem is fixed in software release 5.2(2)CSX. (CSCdm30231)

- Problem channeling with GVRP. A six-port channel with ISL trunking was formed and GVRP was enabled on the channel. An attempt was made to add one additional port with ISL trunking and GVRP enabled to the same admin group of the channel. This failed, as the port failed to become GVRP enabled at the protocol level. NVRAM saved the GVRP status of the port as enabled causing an inconsistency between PAgP and the NVRAM configuration. Although the port channeling parameters look the same between the seventh port and the existing channel, the seventh port cannot join the channel. Disabling GVRP on the existing channel and the new port cleans up the inconsistencies between PAgP and NVRAM and the new port can be added to the channel. This problem is fixed in software release 5.2(2)CSX. (CSCdm32448)

- The supervisor engine might reset after configuring a port channel on the MSM. This problem might occur if the previous MSM configuration was cleared a few seconds earlier using the **clear config** *mod_num* command. This problem is fixed in software release 5.2(2)CSX. (CSCdm33830)

- The spanning tree uplinkfast feature might not converge fast enough or is not converging at all. This problem is fixed in software release 5.2(2)CSX. (CSCdm26273)

- On some GBICs shipped with the switch, when a port is disabled and then enabled, the link might be lost. Some GBICs also might lose link after a power-cycle. This problem is fixed in software release 5.2(2)CSX. (CSCdm33296)

- When ports on the 48-Port 10/100TX Switching modules (WS-X6248-RJ-45 and WS-X6248-TEL) are disabled the **show port flowcontrol** command shows that the port's flow controls are operationally on. This problem is fixed in software release 5.2(2)CSX. (CSCdm29087)

Open and Resolved Caveats in Software Release 5.2(1)CSX

This section describes open and resolved caveats in supervisor engine software release 5.2(1)CSX.

Open Caveats in Software Release 5.2(1)CSX

This section describes open caveats in supervisor engine software release 5.2(1)CSX:

- Changing the console port baud rate from 19,200 to 38,400 incorrectly sets the console port to 9600 baud. After a reset, the console port baud rate is 38,400. Changing the rate to 38,400 from any other setting works correctly. (CSCdk86876)

- In systems with redundant supervisor engines, occasionally during bootup or after a switchover to the redundant supervisor engine, a bus ASIC sequence error syslog message is reported to the console as follows:

  ```
  %SYS-1-MOD_SEQMISMATCH:Bus asic sequence mismatch occurred on module 8
  ```

  This message might be generated for some or all installed modules. Ignore this message. (CSCdm01334)

- If the software image on the MSM is not bootable, contact Cisco's Technical Assistance Center (TAC) at 800 553-2447, 408 526-7209, or tac@cisco.com. This problem is fixed in software release 5.2(2)CSX. (CSCdm03564)

- If the switch is in VTP client mode, entry of a **copy** *device:filename* **config** command may generate messages about nonexistent VLANs. Wait until the **show vlan** command displays the VLANs and then enter the **copy** command again. This problem is fixed in software release 5.3(1)CSX. (CSCdm07337)

- When the last port in a VLAN that is actively participating in GMRP gets removed, the switch might experience a watchdog exception or a TLB exception. This problem is fixed in software release 5.2(2)CSX. (CSCdm11116)

- If protocol filtering is configured for an EtherChannel before the channel forms, it works correctly. If you configure protocol filtering after the channel has formed, it may not work correctly for transmitted traffic. This problem is fixed in software release 5.2(2)CSX. (CSCdm16439)

- Do not configure any module so that the number of GVRP-enabled ports, including the individual physical ports in GVRP-enabled EtherChannels, times the number of VLANs on the module, exceeds 720. This problem is fixed in software release 5.3(1)CSX. (CSCdm18614)

- On switches with more than 100 VLANs, after removing a module or entering a **set module power down** command, wait at least 60 seconds before putting the module back into service, either by reinserting it or by entering a **set module power up** command. This problem is fixed in software release 5.2(2)CSX. (CSCdm19125)

- The Multilayer Switch Module (MSM) is not supported as a SPAN source port. Configuring the MSM as a SPAN source port generates a "Failed to configure source port" message. If you configure the MSM as a SPAN source port, all subsequent SPAN source port configuration commands for that SPAN session generate the same message until you remove the MSM from the source port list with a **set span disable** *mod_num/port_num* command. This problem is fixed in software release 5.3(1)CSX. (CSCdm20365)

- The supervisor engine software incorrectly allows configuration of an MSM as a SPAN destination port. When configured as a SPAN destination port, the MSM ignores the SPAN traffic. If you configure an MSM as a SPAN destination port, remove it from the destination port list with a **set span disable** *mod_num/port_num* command. This problem is fixed in software release 5.2(2)CSX. (CSCdm20714)

- When the SPAN destination port is a trunk port, the encapsulation matches the trunk type: ISL or 802.1Q. When the SPAN destination port is an access port, the default encapsulation is 802.1Q. The default encapsulation cannot be changed on Gigabit Ethernet access ports used as a SPAN destination. To disable 802.1Q encapsulation on other ports, enter a **set trunk** *mod_num/port_num* **off** command before entering a **set span** command. This problem is fixed in software release 5.2(2)CSX. (CSCdm20968)

- On EtherChannels between 10/100 Ethernet switching modules, occasionally after changing the speed of the EtherChannel ports from 10 Mbps to 100 Mbps or 100 Mbps to 10 Mbps, the channel may form with fewer ports or multiple channels may form. To restore the original EtherChannel configuration, disable all the ports in the EtherChannel and then enable them. This problem is fixed in software release 5.2(2)CSX. (CSCdm22352)

- With redundant supervisor engines, after switch over to the standby supervisor engine, SNMP applications on network management systems fail when accessing cdpCacheTable (1.3.6.1.4.1.9.9.23.1.2.1). This problem is fixed in software release 5.2(2)CSX. (CSCdm22434)

- When you turn off the power on any module, you cannot turn the power back on through SNMP. The workaround is to use the CLI command **set module power up** *mod_num*. This problem is fixed in software release 5.3(1)CSX. (CSCdm23288)

- On 10/100 and 100 Mbps Ethernet switching modules with one or more EtherChannel trunks, after entering **set module power down** and **set module power up** commands, occasionally the spanning tree state is "not connected" for all but VLAN 1. To restore connectivity, reset the module. This problem is fixed in software release 5.2(2)CSX. (CSCdm23329)

- If IGMP is enabled, when a port in an EtherChannel to the MSM gets disabled, the switch stops forwarding IP multicast traffic in groups learned on the switch to the MSM. To restore transmission of IP multicast traffic to the MSM, disable and then enable the channel. This problem is fixed in software release 5.2(2)CSX. (CSCdm24673)

Resolved Caveats in Software Release 5.2(1)CSX

This section describes resolved caveats in supervisor engine software release 5.2(1)CSX:

- In some cases, if you change the VLAN assignment of ports in a Fast EtherChannel, some ports are placed in the "errdisable" state and the channel is not renegotiated. The correct behavior is that the channel is torn down and renegotiated. This problem is fixed in software release 5.2(1)CSX. (CSCdk32807)

- Under some circumstances, several ports might incorrectly be assigned the same ifIndex value (you can see the ifIndex values for ports using the show port command). If multiple ports share an ifIndex value, when you change the configuration on one port other ports with the same ifIndex value might be affected. If this problem occurs, clear the switch configuration using the **clear config all** command (make sure you back up your switch configuration before entering this command or your configuration will be lost) and reset the switch. This problem is fixed in software release 5.2(1)CSX. (CSCdk74506)

- In systems with redundant supervisor engines, occasionally during bootup or after a switchover to the redundant supervisor engine, a switching bus sequence error syslog message is reported to the console as follows:

```
%SYS-1-MOD_SEQERROR:Switching bus sequence error occurred on module 8
```

This message might be generated for some or all installed modules. Ignore this message. This problem is fixed in software release 5.2(1)CSX. (CSCdk81972)

- Occasionally, when you remove an NTP server using the **clear ntp server** command, the removed server is not removed from the configuration. The workaround is to reset the switch. This problem is fixed in software release 5.2(1)CSX. (CSCdk84025)

- In some cases, entering the **show cdp neighbors detail** command causes the switch to generate "alignment correction" syslog messages. These messages do not affect the functionality of the switch. This problem is fixed in software release 5.2(1)CSX. (CSCdk85671)

- Occasionally, attempts to create or modify a VLAN fail with this message:

```
Vlan configuration failed (41)
```

The workaround is to reset the switch. This problem is fixed in software release 5.2(1)CSX. (CSCdk88280)

- When a switching module temperature sensor exceeds its minor threshold, the module's Status LED stays green; the Status LED should go to orange. When a switching module temperature sensor exceeds its major threshold, the module's Status LED shows green, red, and then stays green; the Status LED should go to red. This problem is fixed in software release 5.2(1)CSX. (CSCdk92667)

- If you configure an EtherChannel between a Catalyst 6000 or 6500 series switch and a Catalyst 5000 series switch, if the EtherChannel formed from ports in **desirable** mode, a memory leak occurs on the Catalyst 6000 or 6500 series switch. To avoid the problem, use **on** mode. This problem is fixed in software release 5.2(1)CSX. (CSCdk93430)

- If the system message logging level is set to 7 for all facilities, then entering the show logging buffer command can cause an exception error, causing the switch to reset. This problem is fixed in software release 5.2(1)CSX. (CSCdk93930)

- On 10/100 or 100 Mbps Ethernet switching modules with multiple ISL trunks, if one or more trunks goes down, then other ISL trunk ports on the module might not be able to switch ISL frames longer than 1,443 bytes until all trunks are operational. This problem is fixed in software release 5.2(1)CSX. (CSCdm10189)

- After a module is reset, the MIB objects under etherStatsEntry (1.3.6.1.2.1.16.1.1) for the module are removed from etherStatsTable (1.3.6.1.2.1.16.1). To restore the entries, enter **set snmp rmon disable** and **set snmp rmon enable** commands. This problem is fixed in software release 5.2(1)CSX. (CSCdm10685)

- Occasionally, an exception may occur if an entry in usrHistoryControlTable (1.3.6.1.2.1.16.18.1) is usrHistoryControlBucketsRequested (1.3.6.1.2.1.16.18.1.1.3) multiplied by usrHistoryControlObjects (1.3.6.1.2.1.16.18.1.1.2) with a result greater than or equal to 429385320. This problem is fixed in software release 5.2(1)CSX. (CSCdm11328)

- An SNMP query that accesses portTopNControlTable (1.3.6.1.4.1.9.5.1.20.1) or portTopNTable (1.3.6.1.4.1.9.5.1.20.2) where portTopNControlIndex (1.3.6.1.4.1.9.5.1.20.1.1.1) has an out-of-range value (the valid range is 1 through 5) occasionally causes a TLB exception. This problem is fixed in software release 5.2(1)CSX. (CSCdm13058)

- The trapDestOwner MIB object (1.3.6.1.2.1.16.19.13.1.5) is limited to 20 characters. This problem is fixed in software release 5.2(1)CSX (the new limit is 128 characters). (CSCdm17939)

Open Caveats in Software Release 5.1(1)CSX

This section describes caveats for Catalyst 6000 family software release 5.1(1)CSX.

- In systems with redundant supervisor engines, occasionally, during bootup or after a switchover to the redundant supervisor engine, a switching bus sequence error syslog message is reported to the console as follows:

```
%SYS-1-MOD_SEQERROR:Switching bus sequence error occurred on module 8
```

  This message might be generated for some or all installed modules. Ignore this message. This problem is fixed in software release 5.2(1)CSX. (CSCdk81972)

- When a switching module temperature sensor exceeds its minor threshold, the module's Status LED stays green; the Status LED should go to orange. When a switching module temperature sensor exceeds its major threshold, the module's Status LED shows green, red, and then stays green; the Status LED should go to red. This problem is fixed in software release 5.2(1)CSX. (CSCdk92667)

- When you turn off the power on any module, you cannot turn the power back on through SNMP. The workaround is to use the CLI command **set module power up** *mod_num*. This problem is fixed in software release 5.3(1)CSX. (CSCdm23288)

Troubleshooting

This section describes troubleshooting guidelines for the Catalyst 6000 family switch configuration and is divided into the following subsections:

Note   Please refer to the *Release Notes for Catalyst 6000 Family Multilayer Switch Feature Card—Cisco IOS Release 12.0(3)XE* publication for information about how caveat CSCdm83559 affects the MLS feature.

System Troubleshooting

This section contains troubleshooting guidelines for system-level problems:

- When the system is booting and running power-on diagnostics, do not reset the switch.

- After you initiate a switchover from the active supervisor engine to the standby supervisor engine, or when you insert a redundant supervisor engine in an operating switch, always wait until the supervisor engines have synchronized and all modules are online before you remove or inserting modules or supervisor engines or perform another switchover.

- After you download a new Flash image, the next reboot might take longer than normal if Erasable Programmable Logic Devices (EPLDs) on the supervisor engine need to be reprogrammed. Whether this happens depends on which software version was running on the supervisor engine before the download and which software version is downloaded. This can add up to 15 minutes to the normal reboot time.

- If you have a port whose port speed is set to **auto** connected to another port whose speed is set to a fixed value, configure the port whose speed is set to a fixed value for half duplex. Alternately, you can configure both ports to a fixed-value port speed and full duplex.

Module Troubleshooting

This section contains troubleshooting guidelines for module problems:

- If the Catalyst 6000 or 6500 series switch detects a port-duplex misconfiguration, the misconfigured switch port is disabled and placed in the "errdisable" state. The following syslog message is reported to the console indicating the misconfigured port has been disabled due to a late collision error.

```
SYS-3-PORT_COLL:Port 8/24 late collision (0) detected
%SYS-3-PORT_COLLDIS:Port 8/24 disabled due to collision
%PAGP-5-PORTFROMSTP:Port 8/24 left bridge port 8/24
```

  Reconfigure the port-duplex setting and use the **set port enable** command to reenable the port.

- When you hot insert a module into a Catalyst 6000 or 6500 series chassis, be sure to use the ejector levers on the front of the module to seat the backplane pins properly. Inserting a module without using the ejector levers might cause the supervisor engine to display incorrect messages about the module. For module installation instructions, refer to the *Catalyst 6000 Family Module Installation Guide*.

- Whenever you connect a Catalyst 6000 or 6500 series port that is set to autonegotiate to an end station or another networking device, make sure that the other device is configured for autonegotiation as well. If the other device is not set to autonegotiate, the Catalyst 6000 or 6500 series switch autonegotiating port will remain in half-duplex mode, which can cause a duplex mismatch resulting in packet loss, late collisions, and line errors on the link.

VLAN Troubleshooting

This section contains troubleshooting guidelines for VLAN problems:

Note Catalyst 6000 and 6500 series switches do not support ISL-encapsulated Token Ring frames. To support trunked Token Ring traffic in your network, make trunk connections directly between switches that support ISL-encapsulated Token Ring frames. When a Catalyst 6000 or 6500 series switch is configured as a VTP server, you can configure Token Ring VLANs from the switch.

Catalyst 6000 family switches ship with trunking-capable ports in a nontrunking state and the Dynamic Trunking Protocol (DTP) feature in the **auto** mode. In this mode, if a port sees a DTP **on** or DTP **desired** frame, it transitions into trunking state. Although DTP is a point-to-point protocol, some internetworking devices might forward DTP frames. To avoid connectivity problems that might be caused by a Catalyst 6000 or 6500 series switch acting on these forwarded DTP frames, do the following:

- For ports connected to non-Catalyst 6000 or 6500 series devices in which trunking is not currently being used, configure trunk-capable Catalyst 6000 and 6500 ports to **off** by entering the **set trunk** *mod_num/port_num* **off** command.

- When manually enabling trunking on a link to a Cisco router, use the **set trunk** *mod_num/port_num* **nonegotiate** command. The **nonegotiate** keyword is available in Catalyst 6000 and 6500 supervisor engine software release 5.1(1)CSX and later that transitions a link into trunking mode without sending DTP frames.

Spanning-Tree Troubleshooting

This section contains troubleshooting guidelines for spanning-tree problems:

The Spanning-Tree Protocol (STP) blocks certain ports to prevent physical loops in a redundant topology. On a blocked port, the Catalyst 6000 or 6500 series switch receives spanning-tree bridge protocol data units (BPDUs) periodically from its neighboring Catalyst 6000 or 6500 series switch. You can configure the frequency with which BPDUs are received by entering the **set spantree hello** command (the default frequency is set to 2 seconds). If a Catalyst 6000 or 6500 series switch does not receive a BPDU in the time period defined by the **set spantree maxage** command (20 seconds by default), the blocked port transitions to the listening state, the learning state, and to the forwarding state. As it transitions, the Catalyst 6000 or 6500 series switch waits for the time period specified by the **set spantree fwddelay** command (15 seconds by default) in each of these intermediate states. Therefore, a blocked spanning-tree port moves into the forwarding state if it does not receive BPDUs from its neighbor within approximately 50 seconds.

Note We do not recommend using the uplinkfast feature (also known as spanning-tree Uplink FastSwitchover) on switches with more than 20 active VLANs. The convergence time might be unacceptably long for a switch with more than 20 active VLANs.

Use the following guidelines to debug STP problems:

- After a switchover from the active to the standby supervisor engine, the uplink ports on the standby supervisor engine take longer to come up than other switch ports.

- Keep track of all blocked spanning-tree ports in each Catalyst 6000 or 6500 series switch in your network. For each of the blocked spanning-tree ports, keep track of the output of the following commands:

> — **show port**—Check to see if the port has registered a lot of alignment, FCS, or any other type of line errors. If these errors are incrementing continuously, the port might drop input BPDUs.
>
> — **show mac**—If the Inlost counter is incrementing continuously, the port is losing input packets because of a lack of receive buffers. This problem can also cause the port to drop incoming BPDUs.

- On a blocked spanning-tree port, check the duplex configuration to ensure that the port duplex is set to the same type as the port of its neighboring Catalyst 6000 or 6500 series switch.

- On trunk ports, make sure that the trunk configuration is set properly on both sides of the link.

- On trunk ports, make sure that the duplex is set to full on both sides of the link to prevent any collisions under heavy traffic conditions.

- On your Catalyst 6000 family switch, ensure that the sum of the logical ports across all instances of spanning tree for different VLANs does not exceed 4000. The sum of all logical ports equals the number of trunks or channels on the switch times the number of active VLANs on that trunk, plus the number of nontrunking ports on the switch.

⚠️ **Caution** When numerous protocol features (such as VTP pruning, Fast EtherChannel, and RMON) are enabled concurrently, the number of supported logical spanning-tree ports are reduced. Also, to achieve these numbers, we recommend that you keep switched traffic off the management VLAN.

Documentation Updates for Software Release 5.3

This section describes caveats for the Catalyst 6000 family software release 5.3 documentation. These changes will be included in the next update to the documentation.

- The following messages are documented in the online version of the *Catalyst 6000 Family System Message Guide*:

```
SYS-5-SUP_SBYLOWPWR:Standby drawing less power. Potential power budget violation at
switchover
SYS-5-SUP_SBYHIGHPWR:Standby drawing more power. System may run over power budget
SYS-1-SYS_OVERPWRRTNG:System drawing more power than the power supply rating
SYS-1-SYS_NORMPWRMGMT:System in normal power management operation
SYS-1-MOD_PWRSPROMFAIL:Power mgmt sprom failure for module [dec]
```

- The **show file** command is documented only in the online version of the *Catalyst 6000 Family Command Reference, Software Release 5.3* publication.

- The **show mls** command displays combined information about the total number of unicast and multicast packets switched. Unicast and multicast traffic statistics are not displayed separately.

- In the QoS chapter of the *Catalyst 6000 Family Software Configuration Guide, Software Release 5.3*, the default transmit queue drop threshold percentages should be:

Transmit queue drop threshold percentages	• Low-priority queue threshold 1: 80%
	• Low-priority queue threshold 2: 100%
	• High-priority queue threshold 1: 80%
	• High-priority queue threshold 2: 100%

- In the QoS chapter of the *Catalyst 6000 Family Software Configuration Guide, Software Release 5.3*, the section "Classification, Marking, and Policing with an L3 Switching Engine" has a note that should be:

Note   With an L3 Switching Engine, the Catalyst 6000 family switches provide QoS only for the Ethertype field values shown in Table 35-2 in Ethernet_II and Ethernet_SNAP frames.

- In the QoS chapter of the *Catalyst 6000 Family Software Configuration Guide, Software Release 5.3*, the last paragraph in the section "Internal DSCP Values" should be:

   For **trust-dscp** and **trust-ipprec** IP traffic, QoS creates a ToS byte from the 6-bit DSCP value (which may equal an IP precedence value) and, for **trust-cos** and **trust-ipprec** traffic, the original two-least-significant bits from the received ToS byte, and sends the byte to the egress port to be written into IP packets. The original two-least-significant bits from the received ToS byte are not preserved except in **trust-dscp** or **untrusted** traffic.

- QoS supports IGMP classification using version 1 four-bit Type fields.

- QoS MAC ACLs that do not include an ethertype parameter match traffic with any value in the ethertype field, which allows MAC-level QoS to be applied to any traffic.

- In the QoS chapter of the *Catalyst 6000 Family Software Configuration Guide, Software Release 5.3*, the last note ("To avoid inconsistent results") in the section "Policing Rules" should be:

Note   You must configure all ACEs that include the same aggregate policing rule to use the same ACE keyword: **trust-dscp**, **trust-ipprec**, **trust-cos**, or **dscp**. If the ACEs use the **dscp** keyword, the DSCP value specified must be the same.

- The QoS chapter of the *Catalyst 6000 Family Software Configuration Guide, Software Release 5.3*, incorrectly documents a **set qos bridged-packet-microflow-policing** command. In all cases, it should be **set qos bridged-microflow-policing**. In the "Enabling Microflow Policing of Nonrouted Traffic" and "Disabling Microflow Policing of Nonrouted Traffic" sections, the *vlan* parameter is shown as being optional, but it is not. The *vlan* parameter must always be supplied.

- For the **set qos bridged-microflow-policing** command, "routed traffic" only refers to traffic being routed by the MSFC when MLS is enabled. To do microflow policing of traffic to and from other routers, enable bridged microflow policing.

- For wildcards in masks, the QoS chapter of the *Catalyst 6000 Family Software Configuration Guide, Software Release 5.3*, incorrectly states "Use zero bits, which need not be contiguous, where you want wildcards." The reverse is true. Use one bits, which need not be contiguous, where you want wildcards.

- In the QoS chapter of the *Catalyst 6000 Family Software Configuration Guide, Software Release 5.3*, in the "Deleting Named ACLs" section:

   — The example command should be **clear qos acl icmp_acl** (there should not be a "1" at the end).

   — Ignore the "Note". You can use the **commit** command on a deleted ACL while the ACL is attached to ports and VLANs, in which case the **commit** command clears the attachments and deletes the ACL.

- The **show qos acl map** command syntax is documented incorrectly in the QoS chapter of the *Catalyst 6000 Family Software Configuration Guide, Software Release 5.3*. It is:

  show qos acl map {**config** | **runtime**} {*acl_name* | *mod_num/port_num* | *vlan* | **all**}

  See the online version of the *Catalyst 6000 Family Command Reference, Software Release 5.3* publication for complete information about the syntax.

- The **show qos maps** command syntax is documented incorrectly in the QoS chapter of the *Catalyst 6000 Family Software Configuration Guide, Software Release 5.3*. It is:

  show qos maps {**config** | **runtime**} [**cos-dscp-map** | **ipprec-dscp-map** | **dscp-cos-map** | **policed-dscp-map**]

  See the online version of the *Catalyst 6000 Family Command Reference, Software Release 5.3* publication for complete information about the syntax.

- In the QoS chapter of the *Catalyst 6000 Family Software Configuration Guide, Software Release 5.3*, in the "Displaying QoS Information" section, the example command is with the **config** keyword, not the **runtime** keyword.

- The QoS chapter of the *Catalyst 6000 Family Software Configuration Guide, Software Release 5.3*, does not include the WRED thresholds defaults, which are: queue type is tx, threshold 1 is 80 percent, threshold 2 is 100 percent, and the low threshold is picked automatically by the system.

Documentation Updates for Software Release 5.2

This section describes caveats for the Catalyst 6000 family software release 5.2 documentation. These changes will be included in the next update to the documentation.

- Some publications incorrectly document the model number of the 48-Port 10/100TX RJ-21 Ethernet switching module. The model number is WS-X6248-TEL.

- The *Catalyst 6000 family Module Installation Guide* incorrectly states that the 48-Port 10/100TX RJ-21 Ethernet switching module (WS-X6248-TEL) interfaces can use either Category 3 or Category 5 UTP cable. The WS-X6248-TEL module RJ-21 connectors **do not** support Category 3 RJ-21 Telco connectors and cabling. Using Category 3 connectors and cabling causes carrier sense errors. **You must use** Category 5 RJ-21 Telco connectors and cables with the WS-X6248-TEL module.

- The *Catalyst 6000 and 6500 Series Quick Software Configuration, Software Release 5.2* publication incorrectly documents the **set port channel** command syntax. The command syntax is:

```
set port channel mod_num/port_num mode {on | off | desirable | auto} [silent | non-silent]
```

- Refer to the *Catalyst 6000 and 6500 Series Software Configuration Guide, Software Release 5.2*, for information about the **set gvrp applicant** command. This command is not in the *Catalyst 6000 and 6500 Series Command Reference, Software Release 5.2*.

- The *Catalyst 6000 and 6500 Series Command Reference, Software Release 5.2* publication contains a *Usage Guideline* that incorrectly limits the **set port negotiation** command to Gigabit Ethernet ports. The command is usable on all ports.

- The "Egress Port Scheduling" section on page 9-5 of the *Catalyst 6000 and 6500 Series Software Configuration Guide, Software Release 5.2*, incorrectly describes allocation of bandwidth between the transmit queues. QoS allocates buffers, not bandwidth.

- The *Catalyst 6000 and 6500 Series Software Configuration Guide, Software Release 5.2*, does not contain documentation for the **set port negotiation** command. Refer to the "Understanding How Port Negotiation Works" section on page 40 and the "Configuring Port Negotiation" section on page 40 for information about port negotiation.

- The Catalyst 6000 and 6500 Series, Software Release 5.2, publications do not include the procedure for uploading a software image through the console port using the xmodem or ymodem procedure. Refer to the "Uploading a System Image Using Xmodem or Ymodem" section on page 41 for the procedure.

- The *Catalyst 6000 family Supervisor Engine Installation Guide* incorrectly states that 1300W and 1000W power supplies can be used in the same chassis. The guide also does not mention configuration restrictions when using the 1300W supply with two Multilayer Switch Modules (MSMs) in a nine-slot chassis. The restrictions are as follows:

Note The 1000W power supply is used in the six-slot chassis; the 1300W supply is used in the nine-slot chassis. Do not use the 1000W supply in the nine-slot chassis.

  — **Nine-Slot Chassis**
    Because the Catalyst 6000 family modules have different power requirements, certain switch configurations require more power than a single power supply can provide. Although the power management feature allows you to power all installed modules with two power supplies, redundancy is not supported in this configuration. Loss of power redundancy (and the need for more than one supply) is only an issue when you are using two MSMs.

    When operating a nine-slot chassis with power redundancy (or a single supply), the only limitations with two MSMs are that you are limited to five 10/100 modules and cannot have a 1000BaseX GBIC module in the remaining slot, as shown in Table 3.

  — **Six-Slot Chassis**
    When operating a six-slot chassis with power redundancy (or a single supply), there are no limitations with two MSMs; the chassis supports two MSMs and any combination of additional modules.

Table 3   Possible Switch Configurations with Two MSMs

Switch Slots	Switch Configuration					
1	Supervisor	Supervisor	Supervisor	Supervisor	Supervisor	Supervisor
2	MSM	MSM	MSM	MSM	MSM	MSM
3	MSM	MSM	MSM	MSM	MSM	MSM
4	10/100[1]	10/100	10/100	10/100	10/100	Any module
5	10/100	10/100	10/100	10/100	Any module	Any module
6	10/100	10/100	10/100	Any module	Any module	Any module
7	10/100	10/100	Any module	Any module	Any module	Any module
8	10/100	Any module[2]	Any module	Any module	Any module	Any module
9	100FX[3] (1000BaseX not allowed)	Any module[3]	Any module[3]	Any module[3]	Any module[3]	Any module[3]

1 The WS-X6248-TEL (10/100) has the same power consumption as WS-X6248-RJ-45 (10/100).
2 Any module = WS-X6224-100FX-MT (100FX) or WS-X6408-GBIC (1000BaseX).
3 Or a redundant supervisor engine in slot 2 (that is, two supervisor engines and two MSMs).

Understanding How Port Negotiation Works

Note   Port negotiation does not involve negotiating port speed. You cannot disable port negotiation with the **set port speed** command.

Port negotiation exchanges flow-control parameters, remote fault information, and duplex information. Configure port negotiation with the **set port negotiation** command. Port negotiation is enabled by default.

The ports on both ends of a link must have the same setting. The link will not come up if the ports at each end of the link are set inconsistently (port negotiation enabled on one port and disabled on the other). Table 4 shows the four possible port negotiation configurations and the resulting link status for each configuration.

Table 4   **Gigabit Ethernet Autonegotiation Configuration and Possible Link States**

Port Negotiation State		Link Status	
Near End[1]	Far End[2]	Near End	Far End
Off	Off	Up	Up
On	On	Up	Up
Off	On	Up	Down
On	Off	Down	Up

1   Near End refers to the local port.
2   Far End refers to the port at the other end of the link.

Configuring Port Negotiation

To enable port negotiation, perform this task in privileged mode:

Task	Command
Step 1 Enable port negotiation.	**set port negotiation** *mod_num*/*port_num* **enable**
Step 2 Verify the port negotiation configuration.	**show port negotiation** [*mod_num*/*port_num*]

This example shows how to enable port negotiation and verify the configuration:

```
Console> (enable) set port negotiation 2/1 enable
Port 2/1 negotiation enabled
Console> (enable) show port negotiation 2/1
Port   Link Negotiation
-----  ----------------
 2/1   enabled
Console> (enable)
```

To disable port negotiation, perform this task in privileged mode:

Task	Command
Step 1 Disable port negotiation.	**set port negotiation** *mod_num*/*port_num* **disable**
Step 2 Verify the port negotiation configuration.	**show port negotiation** [*mod_num*/*port_num*]

This example shows how to disable port negotiation and verify the configuration:

```
Console> (enable) set port negotiation 2/1 disable
Port 2/1 negotiation disabled
Console> (enable) show port negotiation 2/1
Port   Link Negotiation
-----  ----------------
 2/1   disabled
Console> (enable)
```

Uploading a System Image Using Xmodem or Ymodem

When you need a system image on the switch, but the switch does not have network access and you do not have a software image on a Flash PC card, you can upload an image from a local or remote computer (such as a PC, UNIX workstation, or Macintosh) through the console port using the Xmodem or Ymodem protocol.

Xmodem and Ymodem are common protocols used to transfer files and are included in applications such as Windows 3.1 (TERMINAL.EXE), Windows 95 (HyperTerminal), Windows NT 3.5x (TERMINAL.EXE), Windows NT 4.0 (HyperTerminal), and Linux UNIX freeware (minicom).

Xmodem and Ymodem uploads are slow: use them only when the switch does not have network access. You can speed up the transfer by setting the console port speed to 38400 bps.

Xmodem and Ymodem file transfers are performed from the ROM monitor with the following command:

xmodem [**-y**] [**-c**] [**-s** *data-rate*]

In the example, the **-y** option uses the Ymodem protocol; **-c** provides CRC-16 checksumming; and **-s** sets the console port data rate.

Note   See the "ROM Monitor Command-Line Interface" section in the "Command-Line Interfaces" chapter in the *Catalyst 6000 family Software Configuration Guide* for more information about the ROM monitor.

The computer from which you transfer the supervisor engine software image must be running terminal emulation software that supports the Xmodem or Ymodem protocol.

The following procedure shows a file transfer using the Xmodem protocol. To use the Ymodem protocol, include the **-y** option with the **xmodem** command.

Caution   A modem connection from the telephone network to your console port introduces security issues that you should consider before enabling the connection. For example, remote users can dial into your modem and access the switch configuration settings.

Step 1   Place a supervisor engine software image on the computer's hard drive. You can download an image from Cisco Connection Online (CCO; see the "Cisco Connection Online" section on page 44).

Step 2   To upload from a local computer, connect the console port (port mode switch in the *in* position) to a serial port on the computer, using a null-modem cable. The console port speed must match the speed configured on the local computer.

> **Note** If you are transferring from a local computer, you may need to configure the terminal emulation program to ignore RTS/DTR signals.

Step 3 To upload from a remote computer:

(a) Connect a modem to the console port and to the telephone network.

(b) The modem and console port must communicate at the same speed, which can be from 1200 to 38400 bps, depending on the speed supported by your modem. Use the **confreg** ROM monitor command to configure the console port transmission speed.

(c) Connect a modem to the remote computer and to the telephone network and configure it for the same speed as the supervisor engine.

(d) Dial the number of the supervisor engine modem from the remote computer.

Step 4 Enter the **xmodem** command at the ROM monitor prompt in the terminal emulation window:

```
rommon > xmodem -s 38400 -c
```

Step 5 Start an Xmodem or Ymodem send operation with the computer's terminal emulation software. The computer uploads the system image to the supervisor engine. See your terminal emulation software application manual for instructions on how to execute a Xmodem or Ymodem file transfer.

Step 6 After the new image is completely uploaded, the ROM monitor boots it.

> **Note** Uploading an image through the console port does not create an image file on any of the Flash devices. The uploaded image resides only in memory. The image in memory cannot be saved as a file.

Step 7 After the upload, the console port returns to the default baud rate: 9600. If the upload took place at other than 9600 baud, the remote computer's baud rate must be changed back to 9600 baud.

> **Note** Establish network connectivity to the switch to copy an image file from a TFTP server to one of the flash devices.

Documentation Updates for Software Release 5.1

This section describes caveats for the Catalyst 6000 family software release 5.1 documentation. These changes will be included in the next update to the documentation.

- The *Catalyst 6000 and 6500 Series Software Configuration Guide*, Software Release 5.1, page 4-4. Incorrectly includes a description of how to configure the priority level of each port on Ethernet, Fast Ethernet, and Gigabit Ethernet modules using the **set port level** command. This feature has not been implemented on Catalyst 6000 family switches and the **set port level** command is not supported.

- The *Catalyst 6000 and 6500 Series Software Configuration Guide*, Software Release 5.1, page 6-3. Incorrectly lists ISL as the default trunk encapsulation. The default is **negotiate** mode. If both ports are set to **negotiate** mode, the trunk uses ISL encapsulation.

- The *Catalyst 6000 and 6500 Series Software Configuration Guide*, Software Release 5.1, Table 9-1. Receive queue drop threshold default percentages have changed as follows:

  — Threshold 1: 50 percent

  — Threshold 2: 60 percent

  — Threshold 3: 80 percent

  — Threshold 4: 100 percent

- The *Catalyst 6000 and 6500 Series Command Reference*, Software Release 5.1, Table 2-1. Receive queue drop threshold default percentages have changed as indicated above.

- The Catalyst 6000 family software publications incorrectly describe support for IEEE 802.3Z flow control as being only for Gigabit Ethernet ports. 100 Mbps and 10/100 Mbps ports on Catalyst 6000 family switches support IEEE 802.3Z flow control with the **set port flowcontrol receive** *mod_num/port_num* {**off** | **on** | **desired**} command; the ports do not support the **send** mode.

- The *Catalyst 6000 and 6500 Series Supervisor Engine Installation Guide* and the *Quick Installation Guide - Catalyst 6009 and Catalyst 6509* include incorrect settings for the supervisor engine console port mode switch. The correct settings are as follows.

  — Mode 1—Switch in the *in* position. Use this mode to connect a terminal to the console port using the console cable and data terminal equipment (DTE) adapter (labeled "Terminal") that shipped with the switch.

    You can also use this mode to connect a modem to the console port using the console cable and data communications equipment (DCE) adapter (labeled "Modem") that shipped with the switch.

  — Mode 2—Switch in the *out* position. Use this mode to connect a terminal to the console port using the Catalyst 5000 series Supervisor Engine III console cable (not provided).

- The *Catalyst 6000 and 6500 Series Supervisor Engine Installation Guide* incorrectly states that the system ships with a 16-MB Flash PC card (PCMCIA). The 16- and 20-MB Flash PC cards are available as separately orderable items.

- The *Catalyst 6000 and 6500 Series Supervisor Engine Installation Guide*, *Installation Guide*, and *Module Installation Guide* include incorrect switching bandwidths. The correct specifications are:

  — Catalyst 6000 Series: 32 Gbps

  — Catalyst 6500 Series: 32 to 256 Gbps

Additional Documentation

The following documents are available for the Catalyst 6000 family switches:

- *Catalyst 6000 Family Quick Installation Guide*
- *Catalyst 6000 Family Quick Software Configuration*
- *Catalyst 6000 Family Installation Guide*
- *Catalyst 6000 Family Module Installation Guide*

- *Catalyst 6000 Family Software Configuration Guide*
- *Catalyst 6000 Family Command Reference*
- *Catalyst 6000 Family System Message Guide*

Cisco Connection Online

Cisco Connection Online (CCO) is Cisco Systems' primary, real-time support channel. Maintenance customers and partners can self-register on CCO to obtain additional information and services.

Available 24 hours a day, 7 days a week, CCO provides a wealth of standard and value-added services to Cisco's customers and business partners. CCO services include product information, product documentation, software updates, release notes, technical tips, the Bug Navigator, configuration notes, brochures, descriptions of service offerings, and download access to public and authorized files.

CCO serves a wide variety of users through two interfaces that are updated and enhanced simultaneously: a character-based version and a multimedia version that resides on the World Wide Web (WWW). The character-based CCO supports Zmodem, Kermit, Xmodem, FTP, and Internet e-mail, and it is excellent for quick access to information over lower bandwidths. The WWW version of CCO provides richly formatted documents with photographs, figures, graphics, and video, as well as hyperlinks to related information.

You can access CCO in the following ways:

- WWW: http://www.cisco.com
- WWW: http://www-europe.cisco.com
- WWW: http://www-china.cisco.com
- Telnet: cco.cisco.com
- Modem: From North America, 408 526-8070; from Europe, 33 1 64 46 40 82. Use the following terminal settings: VT100 emulation; databits: 8; parity: none; stop bits: 1; and connection rates up to 28.8 kbps.

For a copy of CCO's Frequently Asked Questions (FAQ), contact cco-help@cisco.com. For additional information, contact cco-team@cisco.com.

Note If you are a network administrator and need personal technical assistance with a Cisco product that is under warranty or covered by a maintenance contract, contact Cisco's Technical Assistance Center (TAC) at 800 553-2447, 408 526-7209, or tac@cisco.com. To obtain general information about Cisco Systems, Cisco products, or upgrades, contact 800 553-6387, 408 526-7208, or cs-rep@cisco.com.

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM, a member of the Cisco Connection Family, is updated monthly. Therefore, it might be more current than printed documentation. To order additional copies of the Documentation CD-ROM, contact your local sales representative or call customer service. The CD-ROM package is available as a single package or as an annual subscription. You can also access Cisco documentation on the World Wide Web at http://www.cisco.com, http://www-china.cisco.com, or http://www-europe.cisco.com.

If you are reading Cisco product documentation on the World Wide Web, you can submit comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco. We appreciate your comments.